User Manual v1.5x

NetAnalysis™

Digital Detective Group
PO Box 698 • Folkestone • Kent • CT20 9FW
Telephone +44 (0) 845 224 8892
www.digital-detective.co.uk

DIGITAL DETECTIVE

Digital Detective Group Limited

PO Box 698 ▪ Folkestone ▪ Kent ▪ CT20 9FW ▪ United Kingdom

Sales: +44 (0)845 224 8892

Support: +44 (0)844 330 8892

Table of Contents

Table of Contents 2

Document Revision Information 7

Version History 7

Getting Help 8

Knowledge Base 8

Support Portal 8

Software Version History 8

Introduction 9

Introduction to NetAnalysis™ 9

Introduction to HstEx™ 10

Who this Manual is For 10

Upgrading from Version 1.37 11

Introduction 11

Additional Browser Support 11

Cache Extraction and Page Rebuilding 11

Time Zone Support 12

New Improved Workspace File 12

Internet Explorer Redirect and LEAK Entries 13

HstEx v3 Support 13

Improved Audit Logging 14

Improved Error Handling 14

Improved Option Management 15

Improved Filtering, Keyword and SQL Queries 16

Other Changes 16

NetAnalysis 1.54 New Features 18

What's New 18

Mozilla Firefox 18

Firefox moz-page-thumbs 18

Firefox moz_formhistory 19

Google Chrome 20

History Index YYYY-MM c2body 20

Google Chrome Page Transitions 21

Downloads 22

Microsoft Internet Explorer Visit Count 22

Query Manager 23

Rebuilding and Exporting Filtered Cached Pages (and Objects) 23

Add Bookmark to Multiple Records 24

Web Page Rebuilding 24

HstEx v3.8 New Features 25

What's New 25

Advanced Forensics Format (AFF®) Support 25
Recovery of Deleted Google Chrome v2 - 19 Cache Entries 25
Recovery of Deleted Mozilla Firefox v1 to 12 Cache Entries 25
Logicube Forensic Dossier® E01 Support 26

NetAnalysis Supported Browsers 27
Supported Browser by Version 27

HstEx Supported Browsers 28
Supported Browser by Version 28

Installing NetAnalysis 29
Introduction 29
Operating System Requirements 29
Latest Release 29
Digitally Signed Software 29
Running Setup 30
End User Licence Agreement 31
Selecting Components 32
Default File Locations 36

Installing HstEx 37
Introduction 37
Operating System Requirements 37
Latest Release 37
Digitally Signed Software 37
Running Setup 38
End User Licence Agreement 39
Default File Locations 43

Installing a Licence Key File 44
Static Licence Key Files 44
Licence Key Management Utility 44
Licence Key File Location 44

USB Hardware Dongles 45
Hardware Licence Dongles 45
Installing and Using 45
Upgrading Licences on a USB Dongle 45
Obtaining the Dongle Manager Software 46
Procedure for Updating a USB Dongle 47

Practice Files 49
Sample Data 49
Case Scenario 49

NetAnalysis: A Guided Tour 50
NetAnalysis 50
Main User Interface 50
Main Toolbar 51
Status Bar 53

Column Headers 54
URL Examination Window 62
Cookie Decoder 63
Host List View 64
Decode URL 65
Record Bookmark 66
Audit Log 67
Column Filter Bar 68
Results Window 69

Configuring NetAnalysis 70
Before You Start 70
Import Settings: Time Zone 70
Import Settings: Date Format 71
Import Settings: Restrict Date Range 71
Case Settings: Investigation 72
Case Settings: Case Data Paths 73
Web Page Rebuilding: Extraction Settings 73
Environment: User Interface 74

Time Zone Configuration 75
Introduction 75
Date/Time Values 75
Universal Coordinated Time 75
Daylight Saving and Standard Time 76
How NetAnalysis deals with Time Zones 76
Identification of Suspect Machine Time Zone 77
ControlSets 77
Time Zone Information Sub-Key 78
Dynamic DST 81
SYSTEMTIME Structure 82
Calculating Signed Integer Bias Values 83
ActiveTimeBias 85
Bias Calculations 86
Returning Daylight / Standard Name Values 86
NetAnalysis ActiveBias Column 87
Time Zone Warnings 88
Dealing with Mixed Time Zone Data 90

Location of Browser Data 91
Internet Explorer: Windows XP 91
Internet Explorer: Windows Vista/7 91
Apple Safari: Windows XP 92
Apple Safari: Windows Vista/7 92
Apple Safari: Apple Macintosh OS X 10.6 93
Mozilla Firefox: Windows XP 93
Mozilla Firefox: Windows Vista/7 93
Mozilla Firefox: Apple Macintosh OS X 10.6 93
Mozilla Firefox: GNU/Linux 94
Google Chrome: Windows XP 94
Google Chrome: Windows Vista/7 94

Google Chrome: Apple Macintosh OS X 10.6 94
Google Chrome: GNU/Linux 95
Opera: Windows XP 95
Opera: Windows Vista/7 95
Opera: Apple Macintosh OS X 10.6 95
Opera: GNU/Linux 96

NetAnalysis Quick Start 97
Before You Start 97
Establishing the Suspect Time Zone 97
Setting the Time Zone 98
Importing History Files 99
Importing History from a Folder Structure 99
Saving the Workspace 102

Finding the Evidence 103
Introduction 103
Quick Filter 103
Viewing/Highlighting Keyword Hits 105
Removing a Filter (F5) 105
Find First URL (F7) 105
Keyword Lists (F4) 106
Searching with Logical Operators 107
SQL Query Builder (CTRL + F4) 107
Sorting 108
Tagging 108
Moving Between Tagged Records 109
Filtering Tagged Records 109
Bookmarking 109
Right Click Context Menu 111

Understanding the Evidence 113
Introduction 113
URL 113
Absolute and Relative Paths 115
URL Encoding 116

Web Page Rebuilding 120
Overview 120
Practice Files 120
Importing Cached Content from a Folder Structure 120
Filtering Cached Items 123
Rebuilding an Individual Web Page 127
How Does NetAnalysis Rebuild a Web Page 128
Rebuild Audit 129
Rebuild and Export All Cached Items 130

Reporting 132
Introduction 132
Advanced Report 132

Exporting 135
Introduction 135
Exporting to TSV 135
Exporting to CSV 136
Exporting to HTML 136
Exporting to PDF 136
Exporting to a Database 136

Deleted Data Recovery 137
Introduction 137
HstEx Processing 137
Limitations of Linear Processing 138
Record Based Extraction (RBE) 138
File Based Extraction (FBE) 139
Recommended Forensic Methodology 139

HstEx: A Guided Tour 140
HstEx 140
Main User Interface 140

HstEx Quick Start 142
Before You Start 142
Getting Started 142
Log File 146
HstEx Options 147

Technical Support 149
Introduction 149
Submitting a Bug Report 150
Background Information 150
Check Version History 150
Mandatory Information 151
NetAnalysis Error Log 151
Submitting an Issue 152

Appendix A 154
Keyboard Shortcuts 154

Appendix B 155
Extended ASCII Table 155

List of References 163
Reference Index 163

Document Revision Information

Version History

The release history for this document is shown in Table 1 below. For ease of comparison, the NetAnalysis major version numbers are also shown.

Document	Software	Author	Date	Comments
1.00	1.20	RCW	12 Jul 2002	1st Public Release
1.01	1.27	RCW	25 Nov 2002	Minor update re QDV viewer
1.02	1.36	RCW	22 Aug 2005	Minor update
1.03	1.37	RCW	18 Jan 2009	Final manual for v1.37h
1.04	1.52	RCW	24 Jun 2011	Manual update for v1.5x | HstEx v3.x; obsolete content removed
1.05	1.53	RCW/PDA	04 Nov 2011	Manual rewritten and brought up to date for v1.53
1.06	1.53	RCW	20 Apr 2012	Support URLs updated for new Knowledge Base
1.07	1.54	RCW	15 Jun 2012	Updated for NetAnalysis v1.54 and HstEx v3.8

Table 1

Getting Help

Knowledge Base

The Digital Detective Knowledge Base should be the first port of call for up to date information in relation to our software:

- *http://kb.digital-detective.co.uk*

Support Portal

If you cannot find the answer to your question within the pages of this document or our knowledge base, or if you need assistance in using our software, please feel free to open a support ticket at our support portal (please see Submitting a Bug Report on Page 150).

- *http://support.digital-detective.co.uk*

Please see the chapter on Technical Support on Page 149 for further information.

Software Version History

The software version history and release notes can be found in our knowledge base at:

- NetAnalysis: *http://kb.digital-detective.co.uk/x/LYUU*
- HstEx: *http://kb.digital-detective.co.uk/x/oIAU*

Introduction

Introduction to NetAnalysis™

The forensic examination of digital devices in support of law enforcement and civil investigations is a critical part of the evidence collection process. Almost every crime investigated by the police has an electronic evidence aspect.

Over the last decade and a half, the Internet has consolidated itself as a powerful platform that has changed the way we do business, and the way we communicate.

The capabilities and opportunities provided by the Internet have transformed many legitimate business activities, augmenting the speed, ease, and range with which transactions can be conducted, whilst also lowering many of the costs. Criminals have also discovered that the Internet can provide new opportunities and multiplier benefits for illicit business. The dark side of the Internet involves not only fraud and theft, pervasive pornography, and paedophile rings, but also drug trafficking and criminal organisations that are more intent upon exploitation than the disruption that is the focus of the hacking community [1].

The forensic examination and analysis of user activity on digital devices can be the pivotal point of any criminal or civil case. It is vital for digital forensics investigators to extract this data, analyse it quickly and present the evidence in an understandable format.

More importantly, as a forensic specialist, you need to be sure that the software you use is accurate, can pass your acceptance/validation testing and can correctly recover live and deleted data from a suspect system.

NetAnalysis is the industry leading software for the extraction and analysis of data from Internet browsers. It was developed in 2001 by a digital forensics practitioner working for a police Digital Forensics Unit in the United Kingdom. There are now over 10,000 licensed users worldwide from the law enforcement and civil communities.

NetAnalysis has a host of features to help with your forensic examination such as the ability to import history and cache data from Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari and Opera browsers. NetAnalysis can also rebuild cached pages for offline review and was the first forensic software designed for this purpose. It also has the ability to utilise powerful SQL queries to quickly identify relevant evidence and a number of other tools to assist in the review and decoding process. The forensic suite also includes HstEx, a software tool designed to recover deleted browser artefacts.

Introduction to HstEx™

HstEx is an advanced, Windows-based, multi-threaded, forensic data recovery solution which has been designed to recover deleted browser history and cache data from a variety of source forensic evidence files as well as physical and logical devices.

Specifically designed to work in conjunction with NetAnalysis, this powerful software can recover deleted data from a variety of Internet browsers, whether they have been installed on Windows, Linux or Apple Mac systems.

HstEx supports a number of different source evidence types such as EnCase® e01 (Expert Witness) image files, AccessData® FTK™ Image files or traditional monolithic and segmented dd image files. It also supports direct sector access to physical and logical devices such as hard disks.

HstEx is able to extract browser history and cache records directly from source forensic files enabling the recovery of evidence, not only from unallocated clusters, but also from cluster slack, memory dumps, paging files and system restore points amongst others. It is an extremely powerful tool in your forensic tool-box.

Who this Manual is For

This manual is designed for both corporate and law enforcement forensic examiners who use NetAnalysis and HstEx for the recovery of web browser evidence. It is suitable for individuals at all levels of experience and is focused towards those who wish to learn how to realise the full potential of our software. Depending on where you are on the spectrum of digital forensics experience, this manual can help you in the following ways:

- If you are completely new to browser forensic analysis and NetAnalysis, this manual will give you a solid grounding in the use of the software as well as basic browser analysis practices and methodologies. It will help you understand the different elements of analysing browser artefacts.

- If you are an experienced forensic examiner, this manual integrates common digital forensic practices with the use of the software tool. This helps you see how you can use NetAnalysis to carry out the browser forensic analysis functions you are accustomed to.

- If you are already an experienced NetAnalysis user, this manual will help you better understand the inner workings of NetAnalysis so that you can use it more effectively and it will mean you are better prepared to explain your findings to others, whether these are colleagues, lawyers or a court.

Upgrading from Version 1.37

Introduction

The release of NetAnalysis v1.50, on 23rd March 2010, was a major milestone on our development roadmap. We added new features to increase product stability and reliability as well as making significant improvements to increase the usefulness and functionality of the product.

All of the extraction and analysis engines were completely re-written to take into account new research, and as a result, we are now extracting data which no other currently available tools can extract.

We have added an array of new features to NetAnalysis as well as a number of improvements to the user interface to make it easier to understand the information presented. Web page rebuilding and cache extraction has been completely re-written in addition to enhanced forensic auditing.

Additional Browser Support

Microsoft Vista and Windows 7 have presented a new set of challenges for us all, and this has been mirrored with the changes to Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari and Opera. NetAnalysis has been updated to now support the latest versions of the most popular browsers.

Cache Extraction and Page Rebuilding

The cache extraction and rebuilding engine has also been re-written. The engine is now recursive and supports GZIP compressed data.

When cached items are extracted or web pages rebuilt, the data is exported to an external export folder. The output paths are relative so the entire folder can be moved to different media and still be viewable.

There is also an option to have cached items exported and grouped by extension for easy review. During the page rebuild process, a new audit log file is created. This page details the content of the page and shows how it was rebuilt. It also contains hyperlinks to all of the page elements.

Our HTML/File viewer QDV™ has also been completely re-written with a new HTML rendering engine which is more stable and able to deal with the scripting issues found during page rebuilding.

Time Zone Support

Historically, one of the biggest sources of confusion for users is time zones and timestamps. From v1.50, timestamp analysis has been improved considerably and the secondary date column has been replaced.

NetAnalysis now takes DST (and Dynamic DST) into account rather than just applying an offset bias. It also allows the user to set the exact time zone the suspect system was set to, thereby accurately recreating the date/times.

NetAnalysis will also flag and report any issues it identifies with time zones after the data has been imported. It will identify if the time zone settings are incorrectly set.

There is also an option to leave timestamps unaltered (no conversion applied) for those investigations where the suspect employs multiple time zone changes.

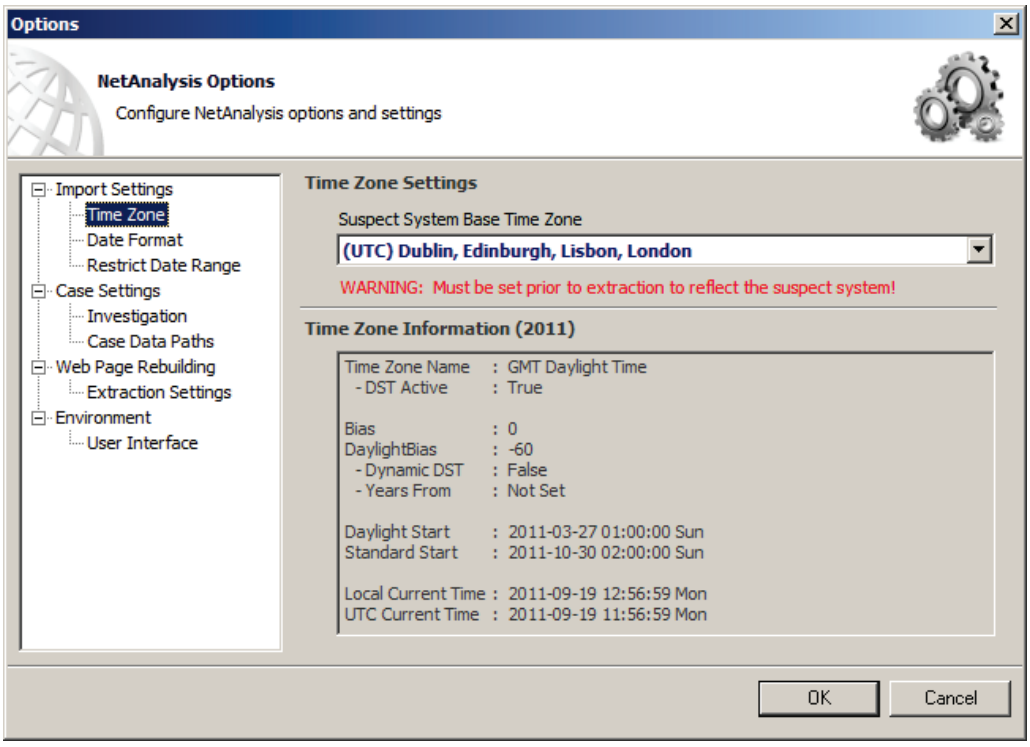


Figure 1

New Improved Workspace File

The NetAnalysis workspace database has been updated and improved. It now contains over 40 new fields.

Internet Explorer Redirect and LEAK Entries

As a result of research and testing, NetAnalysis now has greater support for Redirect and LEAK entries. NetAnalysis is now able to provide date/times for some redirects as well as showing where the user was redirected to (which is displayed in the new Redirect URL column).

LEAK support has been greatly improved with additional date/time reporting and flagging of partial overwrite status. A LEAK entry occurs when Internet Explorer has attempted to remove a cache or cookie file and was unable to do so at that time. It flags the entry as LEAK so that it can remove the item at a later date.

HstEx v3 Support

NetAnalysis v1.5x now supports HstEx v3 extraction files. HstEx can recover deleted browser data from a forensic image or disk. When HstEx v3 files are loaded into NetAnalysis, a new feature identifies the physical location of the Internet history record on the original disk. If you right click on the status bar at this point, the physical sector offset can be copied to the clipboard. This allows the examiner to quickly navigate to that physical location in their forensic tool of choice.

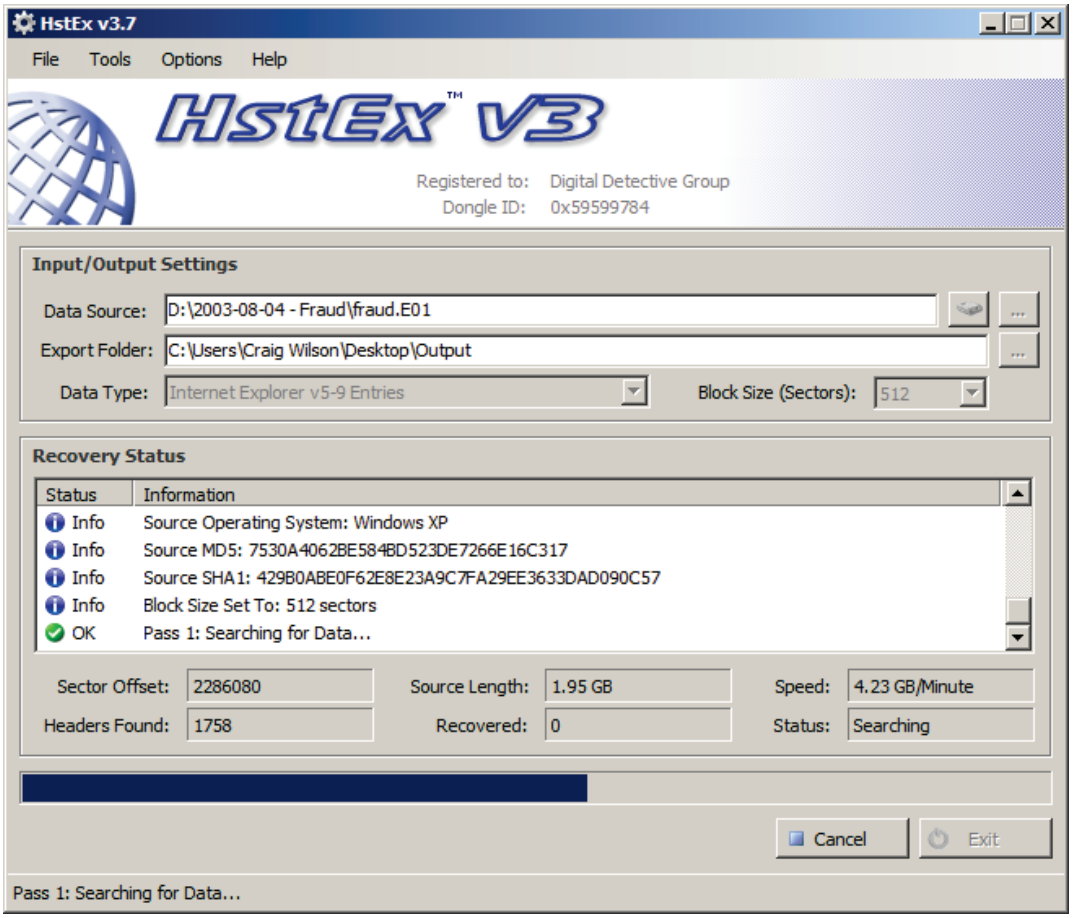


Figure 2

Improved Audit Logging

In previous versions of NetAnalysis, there was a system log which recorded some limited information. In the new version, this has been replaced by an audit log. The audit log will record far more information than previously, to enhance disclosure under legal and regulatory guidelines.

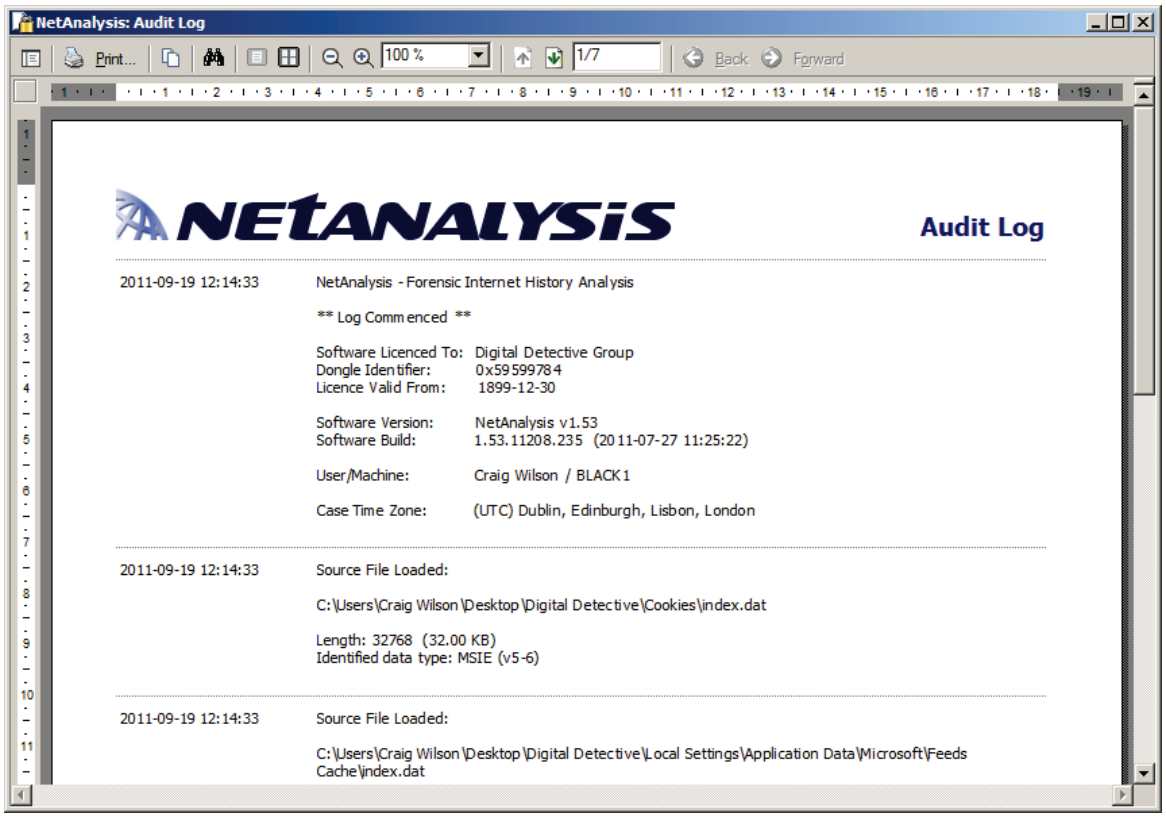


Figure 3

Improved Error Handling

A new error handler has been added to the software. The error reports have comprehensive information regarding each issue, which allows support engineers to quickly identify the cause of a problem. Each session maintains its own error log. The logs can be sent to technical support if required. This will assist in making NetAnalysis a more robust product.

Please ensure when requesting support for an error issue that you include the whole error log. It is not possible to establish the cause of an error by reviewing an error message in isolation.

The full error log will contain vital information which will assist in identifying the issue and will assist the technical support team in quickly finding a solution to your problem.

Error logging can be accessed from Help » Error Reporting. If numerous errors are reported (such as with very corrupt data), the user can disable error reporting for the rest of that session. NetAnalysis will continue to log the errors to the log file. Figure 4 shows the error reporting window.

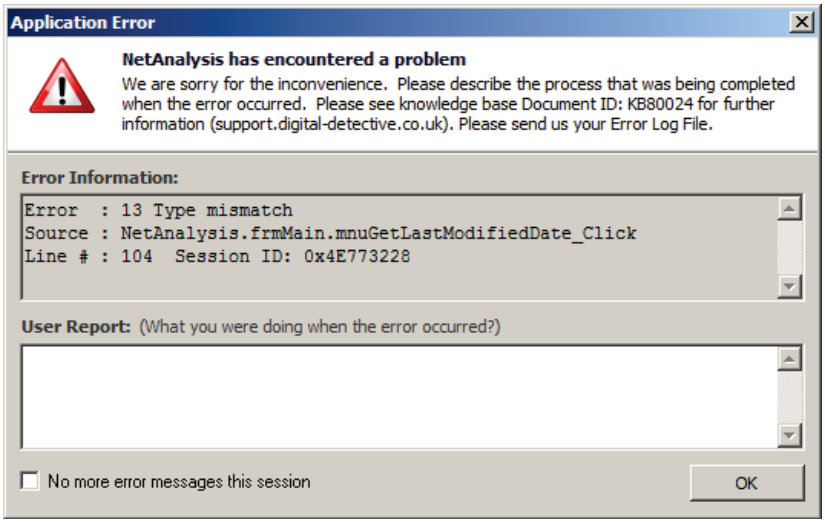


Figure 4

Improved Option Management

NetAnalysis Case and Properties have been merged into one location. All of the software and case properties can now be accessed by selecting Tools » Options from the main menu.

NetAnalysis also remembers many of the options you set as you work. For example, the location of source data and export folders are remembered so they are automatically selected when you use the function again.

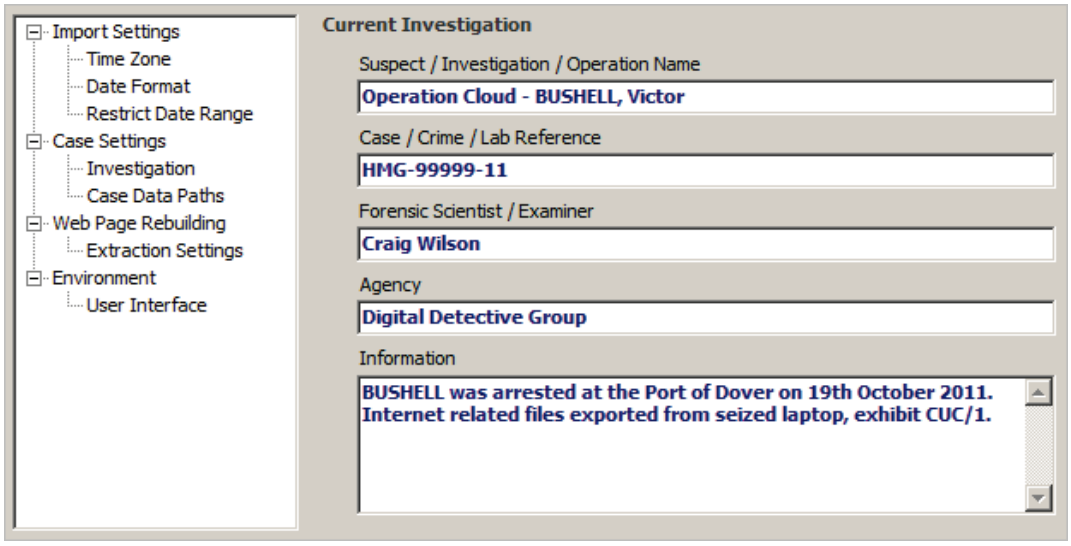


Figure 5

Improved Filtering, Keyword and SQL Queries

NetAnalysis now has some new and improved existing features for record filtering, keyword management and SQL Query building. All of these functions have been re-written to improve usability.

The main searching/filtering form (accessed via the F8 function key) has been redesigned. The Filter Text field is now a dropdown list which remembers the last 15 filters that have been set. If you apply a filter and have the URL View window open, your filter keywords will be highlighted for easy review.

You can now set whether your search string will match any part of the field, match the whole field as an exact match, or only match from the start or end of the field (Figure 6).

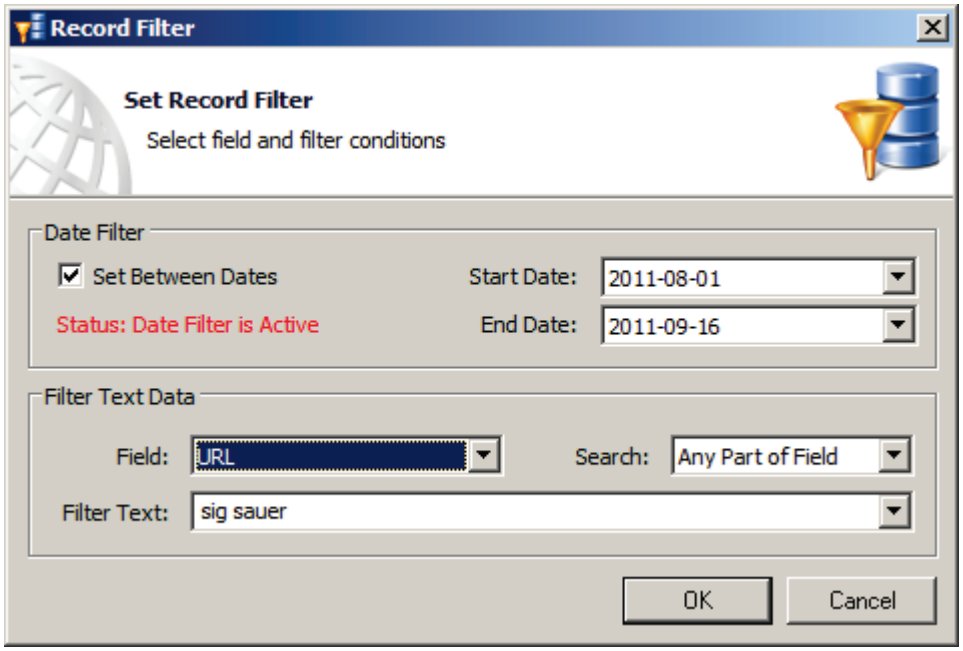


Figure 6

The column sort order is now retained between searches as well as any date specific filtering. You can now easily filter a specific field value by right clicking on the column/record and selecting 'Filter Records by Selected Field Data'.

Other Changes

If you select a live cache entry, you can also select 'Open Containing Folder'. This will take you to the location of the exported cache item and highlight it in Windows Explorer.

The Query Manager has been re-written from scratch to make it easier to use. SQL Queries can easily be saved and exported so they can be shared between users, or archived for later use.

We have also created a number of new example queries to get you started. These queries can be opened from the Query Manager by selecting File » Open. Figure 7 shows the Query Manager with a sample SQL query ready for execution.

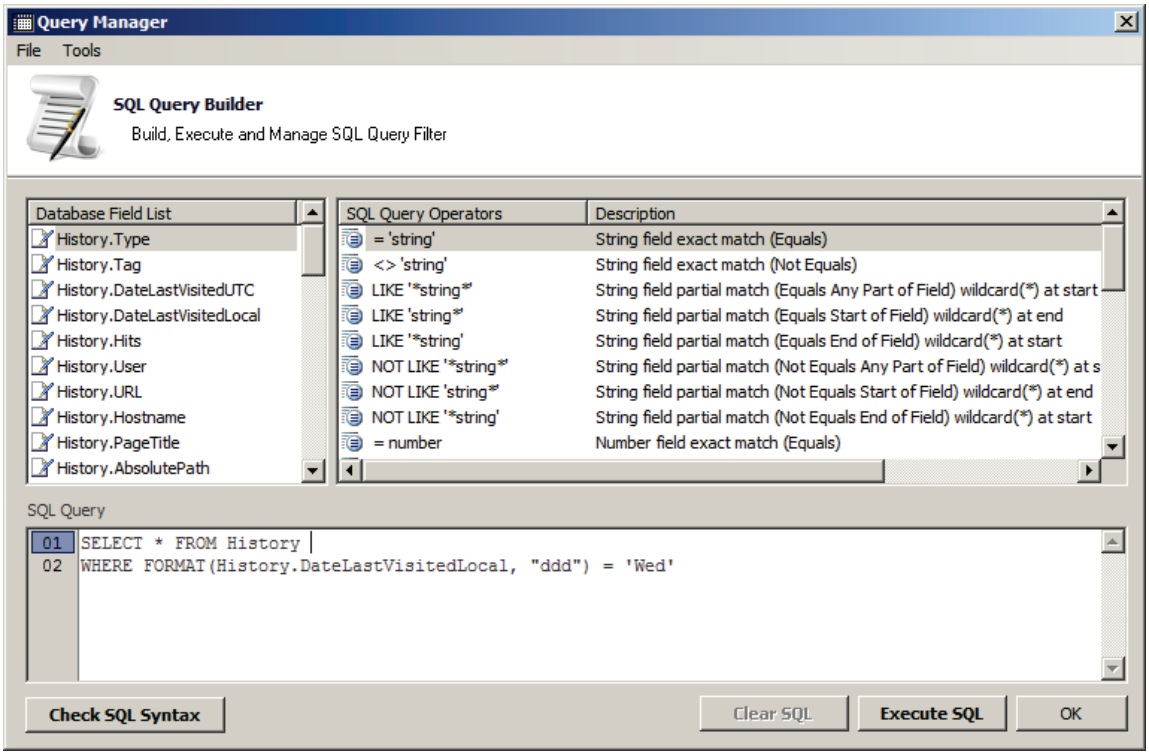


Figure 7

NetAnalysis 1.54 New Features

What's New

In this release, we have added a number of new features and improvements. The corresponding version of HstEx for this release is HstEx v3.8. To allow us to add some new features into HstEx, we have updated the file format. This new format is not backwards compatible with previous versions of NetAnalysis and can only be opened in NetAnalysis v1.54 and above.

Mozilla Firefox

Since the release of NetAnalysis v1.53, we have seen some significant changes in the world of browser forensics. Mozilla has committed to a more aggressive release schedule for the Firefox web browser. There were nearly three years between the launch of Firefox 3 and Firefox 4, however, versions 5 to 12 have been released within a matter of months. This has been a technical challenge from a support point of view as many artefacts have changed during these releases. NetAnalysis now supports all versions of Mozilla Firefox from version 1 through to the current release, Firefox version 12.

Firefox moz-page-thumbs

Firefox v13 will bring a slightly new look to some parts of the browser. Both the New Tab and the Home Page have been redesigned. The New Tab page now has links to your most recently and frequently visited sites which looks more or less just like Opera's Speed Dial, which Chrome also mimics.

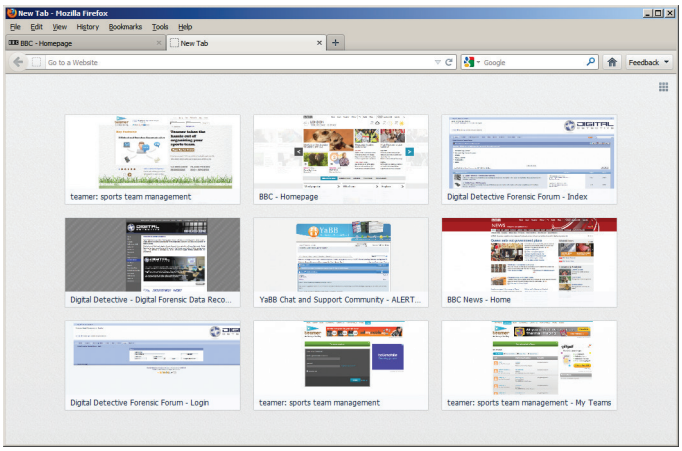


Figure 8

Some of this functionality has been added to Firefox v12 in anticipation of the release of Firefox v13. Whilst Firefox v12 does not show the new Speed Dial page when new tab is selected, the page thumbnails are still saved to the cache when a page is visited. The structure of the URL can be seen in Table 2 below.

Firefox moz-page-thumb cache entry
moz-page-thumb:http://www.browserforensics.com/2011-09-14-Test-Data/visit-count/multi-visit-test.htm

Table 2

We have added additional support to HstEx to recover these entries as part of the Firefox cache recovery process. NetAnalysis v1.54 also supports these cache entries, with the added bonus of being able to extract the page-thumb file (which is usually stored in PNG format).

These thumbnails can easily be exported and reviewed by the forensic examiner. Using the new 'Export/Rebuild Current Filtered Cache Items' feature added to NetAnalysis v1.54, the thumbnail entries can be filtered and then the actual PNG thumbnail files can be exported from the cache. To filter the records, search for "moz-page-thumb" across the imported Firefox v12 records and then select Tools » Export/Rebuild Current Filtered Cache Items. The thumbnail files can then be examined from the 'Extracted Files\PNG' folder.

Firefox moz_formhistory

We have added support to import data from the 'moz_formhistory' table. This contains artefacts relating to web form completion.

https	☐	2012-02-22 11:03:17 Wed	2012-02-22 15:03:17 Wed	1	https://mail.google.com/mail/?shva=1#drafts
https	☐	2012-02-22 11:03:11 Wed	2012-02-22 15:03:11 Wed	1	https://mail.google.com/mail/?shva=1#drafts/135a55f862d94e65
form-hist	☑	**2012-02-22 11:03:00 Wed**	**2012-02-22 15:03:00 Wed**	**1**	**subject : Some research I've done**
file	☐	2012-02-22 11:02:52 Wed	2012-02-22 15:02:52 Wed	1	file:///C:/Users/Alexei_Axe/Downloads/Research.zip

Figure 9

The screen shot in Figure 9 shows an example where the browser user opened a ZIP attachment whilst viewing Google Mail; they then created a draft email using the subject line "Some research I've done".

form-hist	☑	2012-02-22 08:43:30 Wed	2012-02-22 12:43:30 Wed	1	newaccountcaptcha : chavoiava
form-hist	☑	2012-02-22 08:43:30 Wed	2012-02-22 12:43:30 Wed	1	Birthday :
form-hist	☑	2012-02-22 08:43:30 Wed	2012-02-22 12:43:30 Wed	1	SecondaryEmail :
form-hist	☑	2012-02-22 08:43:30 Wed	2012-02-22 12:43:30 Wed	1	ownquestion :
form-hist	☑	2012-02-22 08:43:30 Wed	2012-02-22 12:43:30 Wed	1	LastName :
form-hist	☑	2012-02-22 08:43:30 Wed	2012-02-22 12:43:30 Wed	1	FirstName :
cached	☐	2012-02-22 08:43:30 Wed	2012-02-22 12:43:30 Wed	1	id=4f44a7da&uri=https://accounts.google.com/CreateAccount?service=

Figure 10

The screen shot in Figure 10 shows the user creating a new Google Mail account. It also takes the user through the question and answer fields which are required to create a new account. Although the details in this image have been redacted, you can see the field names which have been completed as part of the process. These artefacts when viewed in context can provide some very interesting information.

Google Chrome

We have added significant extra functionality for Google Chrome artefacts. Chrome maintains a number of SQLite databases for data storage, and NetAnalysis v1.54 now extracts data from most of the significant databases.

History Index YYYY-MM c2body

We have added support for Google Chrome Page Content (c2body). Chrome's history system keeps a full text index for each page the user visits, making it easy to find pages based on their content, not just title and URL. The user's history is exposed through the History page, accessible via the Tools menu, or by pressing Ctrl+H. A user may also directly search their history by typing a search query in the address bar, and selecting the See all pages in history containing [query] item that appears if any results match the entered query.

When a user visits a page, the textual contents (those actually shown on screen) are stripped out and stored in the 'History Index YYYY-MM' database files (one file per month). NetAnalysis v1.54 allows the examiner to extract all of this information in one simple operation. The text files generated have been shown to contain potentially important information including Facebook and webmail data.

The text page content can be extracted by selecting, Tools » Export Google Chrome c2body. Figure 11 shows the extracted text from the visited page.

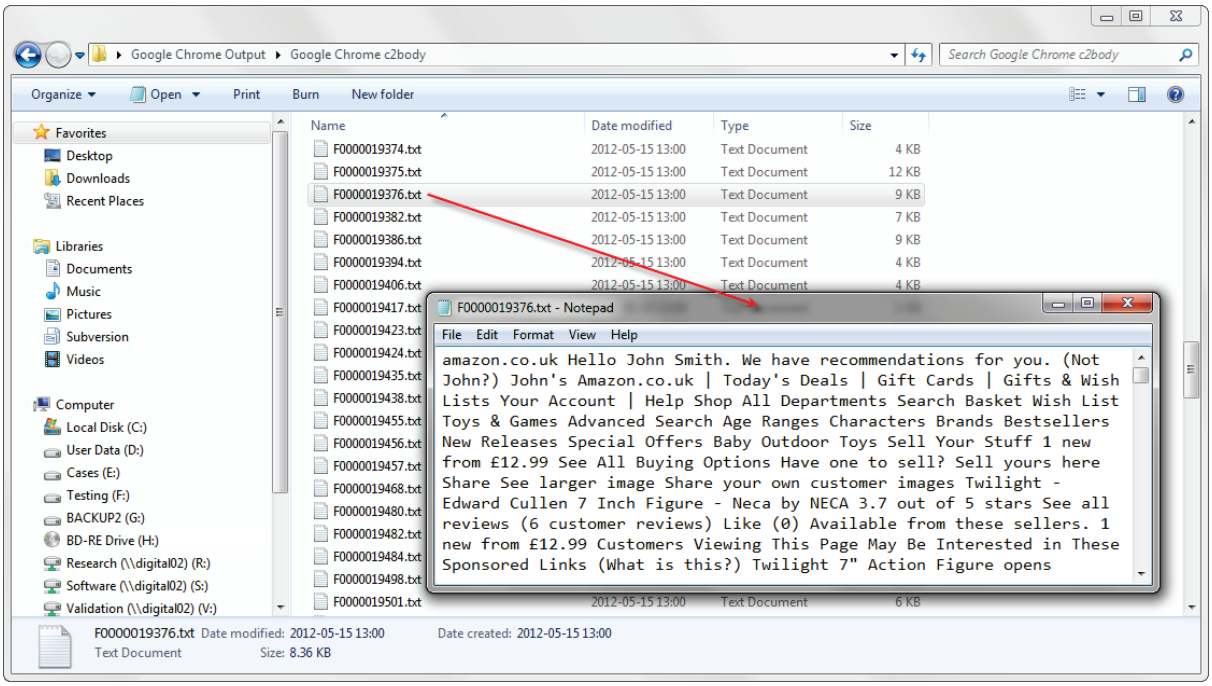


Figure 11

Google Chrome Page Transitions

Google Chrome stores a transition value which identifies the type of transition between pages. These are stored in the history database to separate visits, and are reported by the renderer for page navigations. NetAnalysis now extracts and decodes the page transition values and displays the transitions in the 'Status' column. By examining the page transitions, it is possible to see how a user landed on a page.

Source Offset	Index Type	Browser Version	Status
Index: 6246	History	Google Chrome v0-18 (History)	Page transition: AUTO_SUBFRAME and CHAIN_END and SERVER_REDIRECT
Index: 6267	History	Google Chrome v0-18 (History)	Page transition: AUTO_SUBFRAME and CHAIN_END and SERVER_REDIRECT
Index: 4472	History	Google Chrome v0-18 (History)	Page transition: AUTO_SUBFRAME and CHAIN_START
Index: 4476	History	Google Chrome v0-18 (History)	Page transition: AUTO_SUBFRAME and CHAIN_START
Index: 6396	History	Google Chrome v0-18 (History)	Page transition: AUTO_SUBFRAME and CHAIN_START and CHAIN_END
Index: 6398	History	Google Chrome v0-18 (History)	Page transition: AUTO_SUBFRAME and CHAIN_START and CHAIN_END
Index: 4470	History	Google Chrome v0-18 (History)	Page transition: AUTO_SUBFRAME and SERVER_REDIRECT
Index: 4500	History	Google Chrome v0-18 (History)	Page transition: FORM_SUBMIT and CHAIN_END and SERVER_REDIRECT
Index: 6392	History	Google Chrome v0-18 (History)	Page transition: FORM_SUBMIT and CHAIN_END and SERVER_REDIRECT
Index: 4647	History	Google Chrome v0-18 (History)	Page transition: FORM_SUBMIT and CHAIN_START and CHAIN_END

Figure 12

Downloads

We have also added support for Google Chrome download history. Figure 13 shows the download URL with Figure 14 showing the Download Path, Length and Download Status.

Type	Last Visited [Local]	URL
download	2012-05-16 08:42:24 Wed	http://www.digital-detective.co.uk/software/NetAnalysis-v1.53-win32-1.53.11280.253.zip
download	2012-05-16 08:42:15 Wed	http://www.digital-detective.co.uk/software/HstEx-v3.7-win32-3.7.11207.2.zip
download	2012-05-16 08:42:06 Wed	http://www.digital-detective.co.uk/software/DCode-v4.02a-build-4.02.0.9306.zip

Figure 13

Download Path	Length	Status
C:\Users\Paul Andrews\Downloads\NetAnalysis-v1.53-win32-1.53.11280.253 (1).zip	9200005	State: Complete | Opened: True
C:\Users\Paul Andrews\Downloads\HstEx-v3.7-win32-3.7.11207.2 (1).zip	3945586	State: Complete | Opened: False
C:\Users\Paul Andrews\Downloads\DCode-v4.02a-build-4.02.0.9306.zip	388705	State: Complete | Opened: False

Figure 14

Microsoft Internet Explorer Visit Count

Recent testing has exposed an issue with the accuracy of Internet Explorer hit count values stored in the Master INDEX.DAT file. Normally, the hit count would be stored as a 32bit integer at record offset 0x54 (decimal 84). In many cases, comparing the record value to the hit count returned by Internet Explorer would show a mismatch. In these cases, Internet Explorer has an additional record object which stores an additional visit count.

Testing has shown this additional count object to be accurate and is the value presented by the application. When the additional record object is present, NetAnalysis parses that block and displays that value in the Hits column. The original value stored at offset 0x54 is now displayed in the 'Status' column as can be seen from Figure 15 below.

Hits	URL	Host	Status
2	http://en.wikipedia.org/wiki/Firefox	en.wikipedia.org	* Record Offset 0x54 Count: 478
2	http://www.nero.com/eng/slp-nero-burning-rom11-discount-ssp.html?NeroSID=79ba631a7b533302374f0972c63728ac	www.nero.com	* Record Offset 0x54 Count: 58
2	http://code.google.com/p/mft2csv/wiki/mft2csv	code.google.com	* Record Offset 0x54 Count: 558
2	http://code.google.com/p/mft2csv/downloads/detail?name=MFTRCRD_v2.zip&can=2&q=	code.google.com	* Record Offset 0x54 Count: 543
2	http://www.microsoft.com/getsilverlight/Get-Started/Install/Default.aspx	www.microsoft.com	* Record Offset 0x54 Count: 922

Figure 15

Query Manager

This release has an updated Query Manager with additional features. It is now possible to sort the 'Database Field List' and 'SQL Query Operators' by clicking on the corresponding column header. The 'SQL Query Operators' now have a 'Description' entry which explains the function of the Operator. The Operators have also been re-written to show the full Operator with parameters and wild card characters. This should make it much easier to build and understand your SQL queries. The 'Check SQL Syntax' button has been added as a more convenient way to verify the syntax of a query.

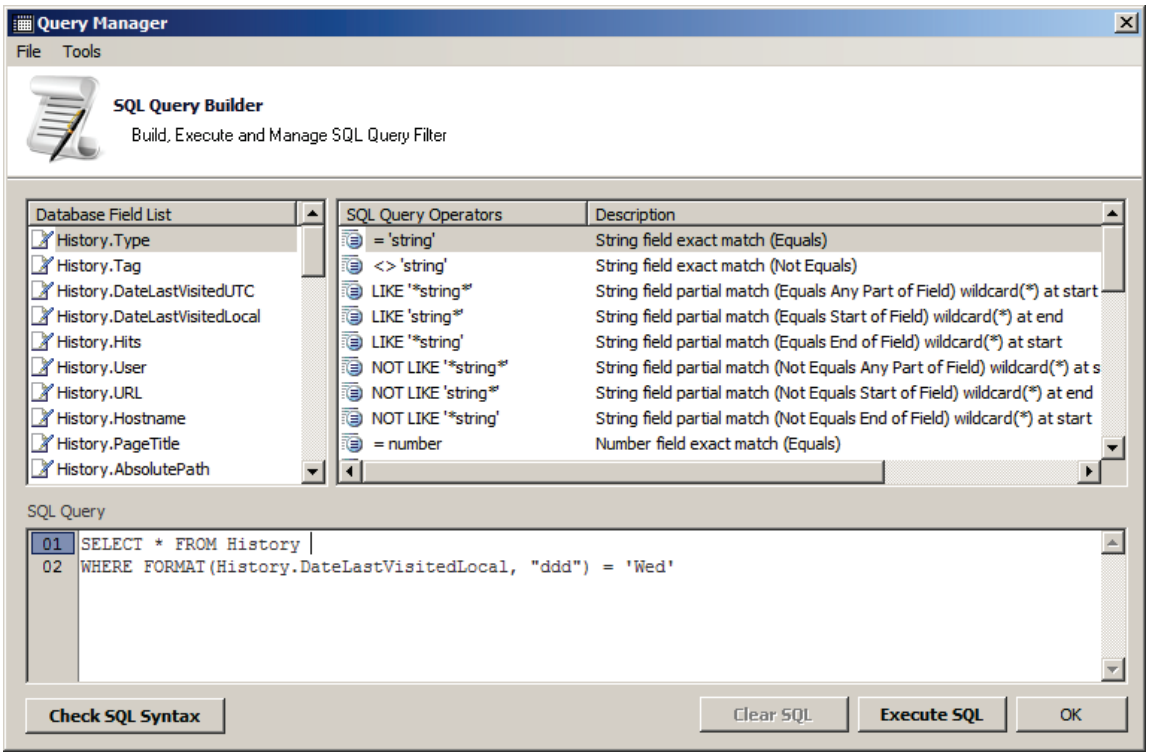


Figure 16

Rebuilding and Exporting Filtered Cached Pages (and Objects)

NetAnalysis has long had the capability to rebuild either single webpages, or the entire cache in one operation. NetAnalysis v1.54 now allows the forensic examiner to rebuild part of the cache. Using the various filtering techniques available, the forensic examiner can generate a targeted subset of the browser data, and then rebuild only the live webpages (or export cached objects) contained within that subset.

For example, if you wanted to export only the moz-page-thumb files, search for "moz-page-thumb" across the imported Firefox v12 records and then select Tools » Export/Rebuild Current Filtered Cache Items. The thumbnail files can then be examined from the "Extracted Files\PNG" folder.

Add Bookmark to Multiple Records

The bookmarking feature in NetAnalysis v1.54 has been enhanced to allow the forensic examiner to bookmark many records with the same bookmark text. The forensic examiner can create a filtered list of specific records, and then apply the same bookmark text to all of these records in one operation. The bookmark column can also be used for filtering, so this functionality is a powerful addition to the armoury.

Web Page Rebuilding

We have enhanced the web page rebuilding engine to make it more robust and provide better results. We have also released v4 of QDV™, our internal web page viewing software. This new version suppresses script errors in web pages, so the forensic examiner will no longer need to cancel multiple error messages when reviewing some rebuilt web pages.

HstEx v3.8 New Features

What's New

In this release we have added some new functionality in terms of source processing and browser support. We have added support for processing data saved in Advanced Forensic Format as well as adding the ability to recover Google Chrome cache records. In addition, we have added support for Logicube Dossier E01 images.

Advanced Forensics Format (AFF®) Support

The Advanced Forensics Format (AFF®) is an extensible open format for the storage of disk images and related forensic metadata. It was developed by Simson Garfinkel and Basis Technology. HstEx now supports the processing of AFF® image files (as well as other forensic formats).

As this version of HstEx supports AFF®, the application implements version 3 of the HstEx file format (HstEx v3.0 - 3.7 uses version 2). The output files from HstEx v3.8 can only be opened in NetAnalysis v1.54+.

Recovery of Deleted Google Chrome v2 - 19 Cache Entries

HstEx version 3.8 now adds the ability to recover live and deleted Google Chrome Cache entries from all source data types. This is a significant addition to the software, as previously, it was only possible to examine live entries, which were still available, on a suspect system. HstEx v3.8 can recover cache entries from Google Chrome browser v2 through to the current release v19.

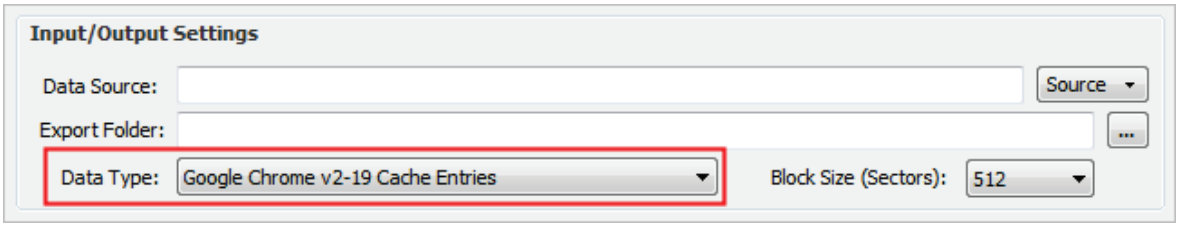


Figure 17

Recovery of Deleted Mozilla Firefox v1 to 12 Cache Entries

Mozilla has committed to a more aggressive release schedule for the Firefox web browser. There were nearly three years between the launch of Firefox 3 and Firefox 4, however, versions 5 to 12

have been released within a matter of months. This has been a technical challenge from a support point of view as many artefacts have changed during these releases. HstEx now supports all versions of Mozilla Firefox cache entries from version 1 through to the current release, Firefox version 12.

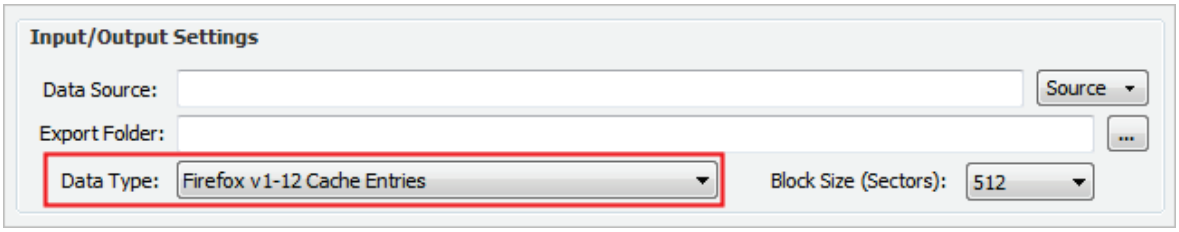


Figure 18

Logicube Forensic Dossier® E01 Support

With HstEx v3.8, we have added support for the E01 files produced by the Logicube Forensic Dossier. Unfortunately, earlier versions of HstEx are unable to load and read the E01 files generated by the Logicube Dossier because of an incompatibility with the metadata fields. Some of the values written to these fields are in a different format than those written by EnCase or FTK Imager. This has now been resolved.

NetAnalysis Supported Browsers

Supported Browser by Version

Table 3 lists the currently supported browsers. Whilst newer browser versions may work, this is the current list we have tested against.

Browser / Version	Information	History	Cache	Rebuild
Microsoft Internet Explorer v3	Client UrlCache MMF Ver 3.2	•	•	•
Microsoft Internet Explorer v4	Client UrlCache MMF Ver 4.7	•	•	•
Microsoft Internet Explorer v5 - 9.0	Client UrlCache MMF Ver 5.2	•	•	•
Mozilla Firefox v1 - 2	Mork DB and Cache Map	•	•	•
Mozilla Firefox v3 - 12	SQLite and Cache Map	•	•	•
Google Chrome v0.2 -19.0	History and Cache	•	•	•
Flock v2	Mozilla based browser	•	•	•
Orca v1	Orca Browser	•	•	•
Avant v7 - 11.9.0.32	Avant Browser (Trident Based Engine)	•	•	•
Sundial up to v4.0.2	Sundial Browser	•	•	•
Netscape Communicator v4.0 - 4.08	Little and Big Endian Versions	•	•	•
Netscape Communicator v4.5 - 4.8	Little and Big Endian Versions	•	•	•
Netscape v6.0 - 6.2.3	Netscape Browser	•	•	•
Netscape v7.0 - 7.2	Netscape Browser	•	•	•
Netscape v8.0 - 8.1.3	Netscape Browser	•	•	•
Netscape v9.0 - 9.0.0.6	Netscape Browser	•	•	•
AOL Browser ARL File	AOL Browser	•	•	•
Opera v4 -11.64	Opera Browser	•	•	•
Yahoo! BT Browser	Yahoo! British Telecom Browser	•	•	•
Apple Safari Windows v3 - 5.1.7	Binary/XML History and Cache.db	•	•	•
Apple Safari Mac OSX v1 - 5.1.7	Binary/XML History and Cache.db	•	•	•
Mozilla / Firefox / Netscape Bookmark	XML Bookmark File	•	N/A	N/A

Table 3

HstEx Supported Browsers

Supported Browser by Version

Table 4 lists the currently supported browsers. Whilst newer browser versions may work, this is the current list we have tested against.

Browser / Version	Information
Microsoft Internet Explorer v4	All INDEX.DAT based records
Microsoft Internet Explorer v5-9	All INDEX.DAT based records
Mozilla Firefox v1-2 File	Firefox v1-2 History / Cache Entries
Mozilla Firefox v1-12 Cache Entries	Firefox v1-12 Cache Entries
Safari (XML) Plist History Entries	Safari XML based PLIST (Early Windows and Apple Mac Versions)
Safari (Binary) Plist History Entries	Safari Binary based PLIST
Google Chrome v2-19 Cache Entries	Google Chrome Browser Cache Entries v2-19
Mozilla / Netscape / Firefox Bookmark Entries	Mozilla based browser Bookmark File
Yahoo! BT Browser History Entries	Yahoo! Browser as provided by British Telecom

Table 4

Installing NetAnalysis

Introduction

The following procedure will guide you through installing NetAnalysis for the first time. Please ensure that you close all other applications before starting.

Operating System Requirements

NetAnalysis has been designed to work on the Microsoft® Windows® platform in either a 32 or 64 bit environment. It has been tested on the following versions of Windows:

- Windows XP
- Server 2003
- Vista
- Windows 7
- Server 2008
- Server 2008 R2

Latest Release

Prior to installing NetAnalysis, please ensure you have obtained the latest release. There is on-going product research and development which provides new features, important updates and bug fixes. Please check the change log for details of those changes.

The release history and change log can be found here:

- *http://kb.digital-detective.co.uk/x/LYUU*

The latest download links for NetAnalysis and HstEx can be found here:

- *http://start.digital-detective.co.uk*

Digitally Signed Software

Software vendors can digitally sign and timestamp the software they distribute. The code signing process ensures the end user knows the digitally signed software is legitimate, comes from a known software vendor and the code has not been tampered with since being published. If the

Authenticode Digital Signature is not valid, or the MD5 hash provided at the point of download does not match, please do not install the software.

All the software products published by Digital Detective have been digitally signed. This ensures that when you use our software, you can verify that it has not been tampered with and is a product developed and released by Digital Detective Group. The following Knowledge Base article explains this further and shows you how to verify the integrity of forensic grade software:

- *http://kb.digital-detective.co.uk/x/u4EU*

Running Setup

Now that you have verified the integrity of the setup file (all the individual executables have also been digitally signed) you can install the software. You will note that each release has been named using the version/build information (see Figure 19).

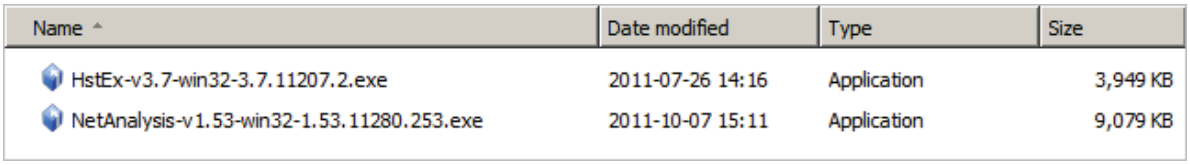


Figure 19

Good forensic practice dictates that you archive each release of NetAnalysis that you use on a forensic case. This ensures that at any time in the future, you can install a specific version and replicate your results. When you run Setup, you will be prompted to select a language. This language selector is for the installation only and does not change the language used by NetAnalysis or HstEx (which is currently English).

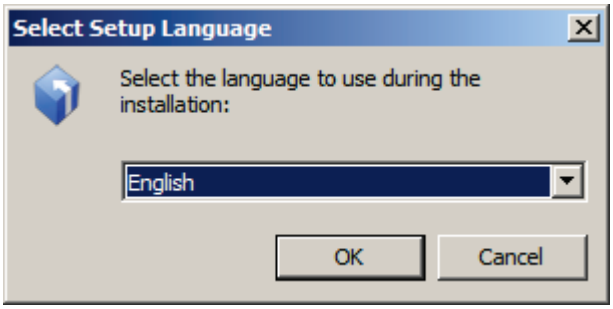


Figure 20

Select the appropriate language and click OK to launch the Setup Wizard (as shown in Figure 21).

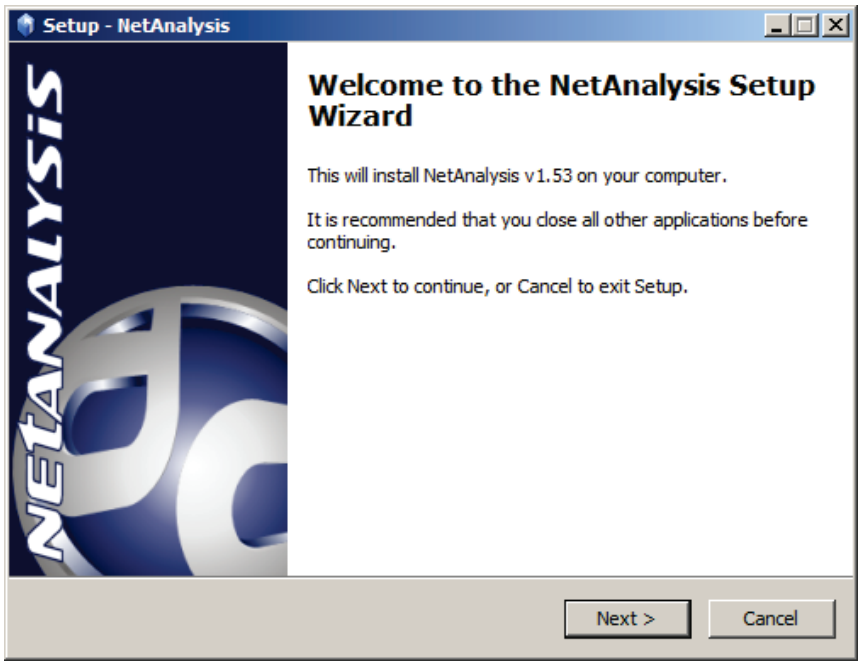


Figure 21

End User Licence Agreement

The next screen (Figure 22) displays the End User Licence Agreement. Please read this carefully. If you wish to review or print a copy of this agreement, it can be found in our knowledge base:

- *http://kb.digital-detective.co.uk/x/flUU*

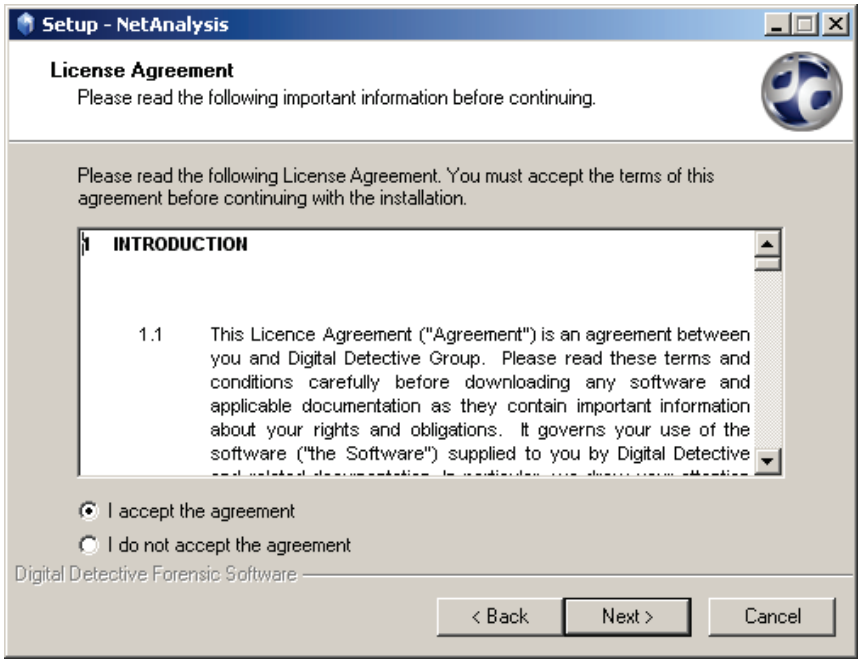


Figure 22

If you accept the agreement, please select the appropriate option and click 'Next'.

The next screen (Figure 23) prompts you to select a location in which to install NetAnalysis. Please note this is a different location from where NetAnalysis v1 - 1.37 was installed.

Version 1.5x can be installed in parallel to previous versions. You will need to do this if you wish to open your old workspace files as they cannot be opened in v1.5x. See the following knowledge base article on workspace files:

- *http://kb.digital-detective.co.uk/x/7IAU*

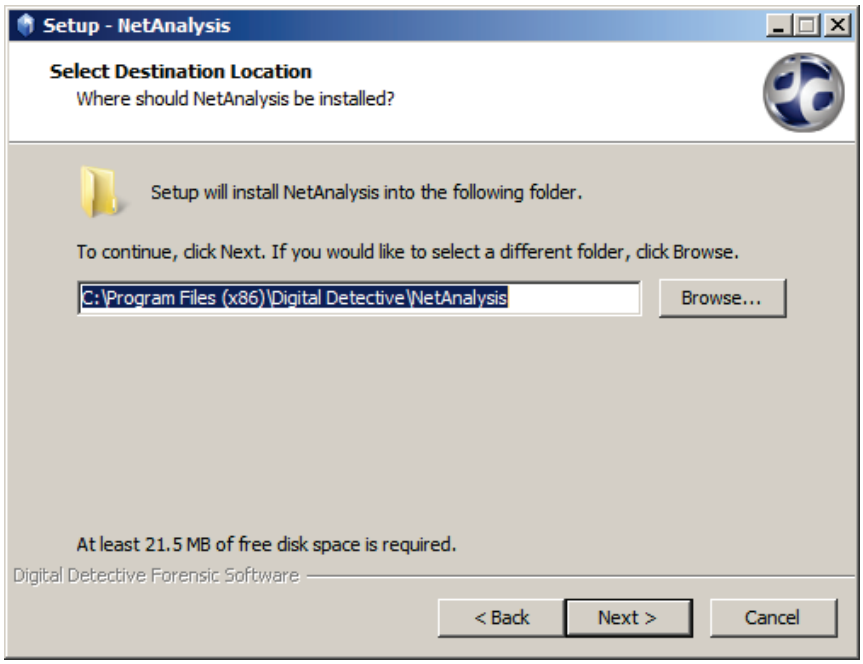


Figure 23

Selecting Components

The next screen (Figure 24) allows you to select which components to install. For a new installation, it is recommended that you install all components.

The Licence Key Management Utility (see the chapter on Installing a Licence Key File on Page 44) is a utility for installing a Static Licence Key File. If you have purchased a USB Dongle Licence, you will not need this utility.

NetAnalysis comes with a number of example SQL filters and Keyword files. These example files will help you become more familiar with building SQL queries and running keyword searches. Select this option if you wish to install these additional components. We recommended that this option is left selected.

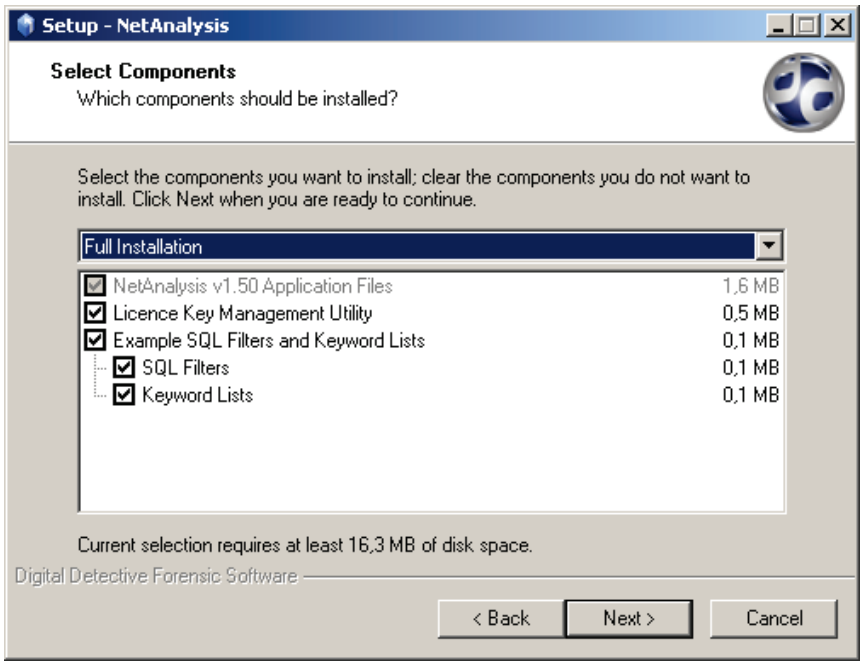


Figure 24

The next screen (Figure 25) shows the location of the Start Menu folder where the icons for the software will be placed. The default location for NetAnalysis is in a folder called Digital Detective. You will find all our products in this location.

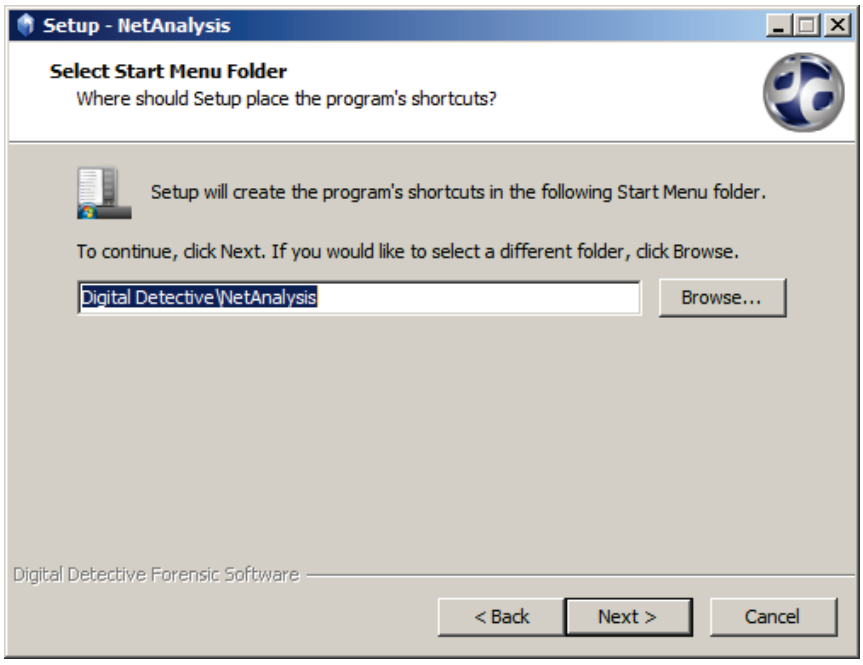


Figure 25

The next screen (Figure 26) shows the additional installation tasks and gives you the option to create icons on your Desktop and/or in the Quick Launch Area.

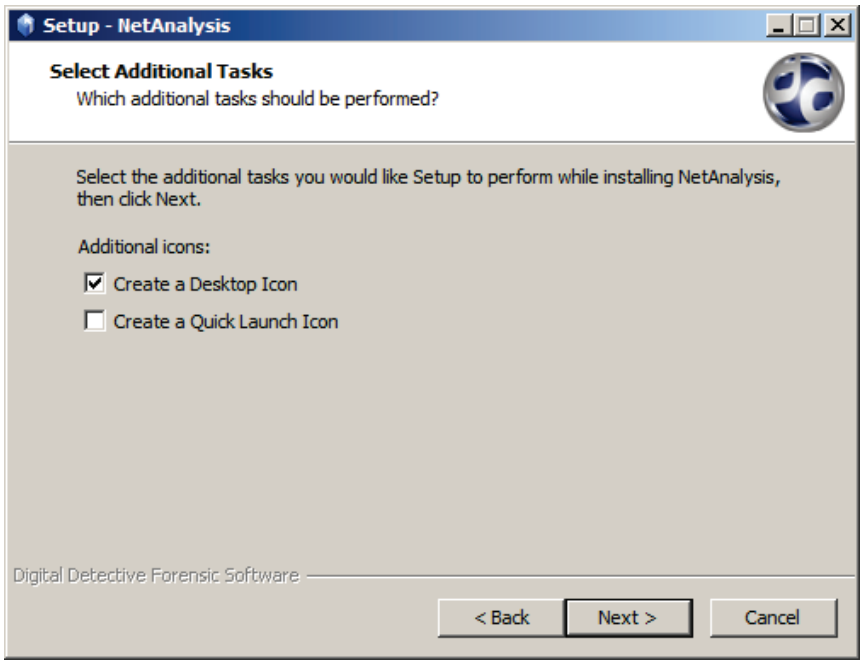


Figure 26

The next screen (Figure 27) shows a summary of the installation tasks prior to launching the installation process.

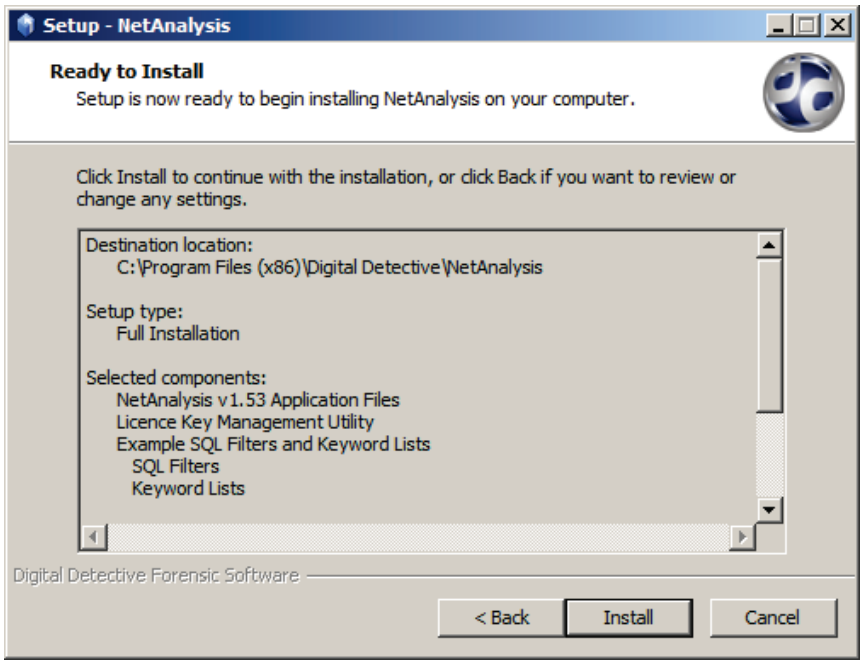


Figure 27

The next screen (Figure 28) shows important information in relation to installing a static Licence Key File or using a USB Dongle.

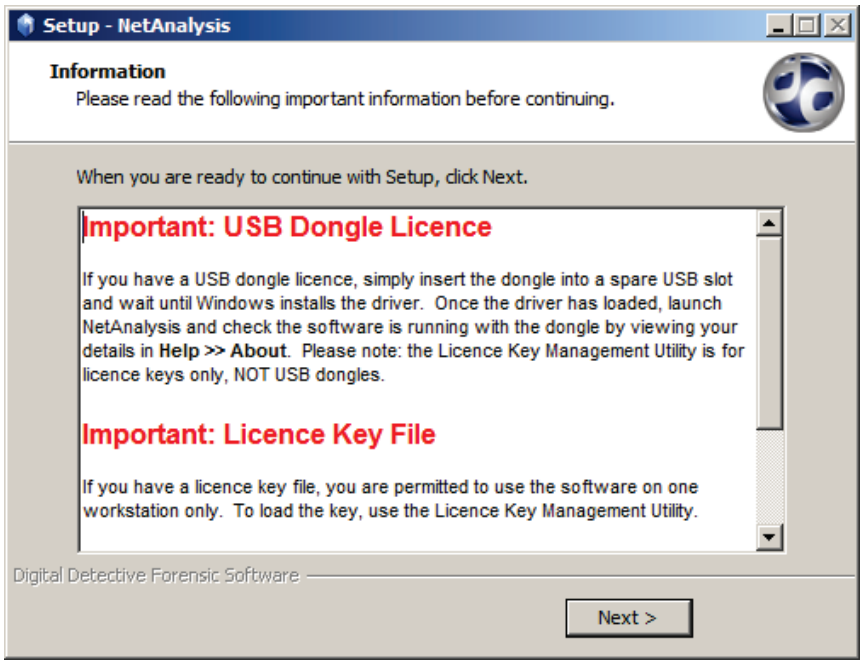


Figure 28

The final screen (Figure 29) shows that the NetAnalysis Setup Wizard has completed. At this point, you may be asked to reboot your workstation. Please ensure this is done before you try and use NetAnalysis.

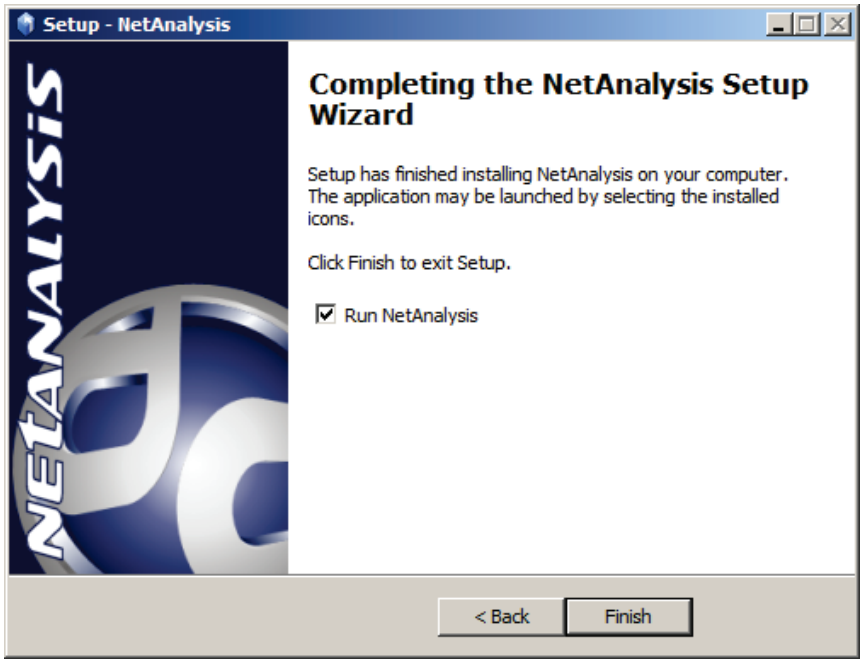


Figure 29

Default File Locations

The default installation folders for NetAnalysis are shown in Table 5 below. As they are in a different location from version 1.20 - 1.37, it is possible to run both versions side by side. You may do this if you wish to access older workspace files.

Operating System	Path
Windows 32 bit	C:\Program Files\Digital Detective\NetAnalysis\
Windows 64 bit	C:\Program Files (X86)\Digital Detective\NetAnalysis\

Table 5

Installing HstEx

Introduction

The following procedure will guide you through installing HstEx for the first time. Please ensure that you close all other applications before starting.

Operating System Requirements

HstEx has been designed to work on the Microsoft® Windows® platform in either a 32 or 64 bit environment. It has been tested on the following versions of Windows:

- Windows XP
- Server 2003
- Vista
- Windows 7
- Server 2008
- Server 2008 R2
- HstEx also requires Microsoft .Net Framework v2

Latest Release

Prior to installing HstEx, please ensure you have obtained the latest release. There is on-going product research and development which provides new features, important updates and bug fixes. Please check the change log for details of those changes.

The release history and change log can be found here:

- *http://kb.digital-detective.co.uk/x/oIAU*

The latest download links for NetAnalysis and HstEx can be found here:

- *http://start.digital-detective.co.uk*

Digitally Signed Software

Software vendors can digitally sign and timestamp the software they distribute. The code signing process ensures the end user knows the digitally signed software is legitimate, comes from a known software vendor and the code has not been tampered with since being published. If the

Authenticode Digital Signature is not valid, or the MD5 hash provided at the point of download does not match, please do not install the software.

All the software products published by Digital Detective have been digitally signed. This ensures that when you use our software, you can verify that it has not been tampered with and is a product developed and released by Digital Detective Group. The following Knowledge Base article explains this further and shows you how to verify the integrity of forensic grade software:

- *http://kb.digital-detective.co.uk/x/u4EU*

Running Setup

Now that you have verified the integrity of the setup file (all the individual executables have also been digitally signed) you can install the software. You will note that each release has been named using the version/build information (see Figure 30).

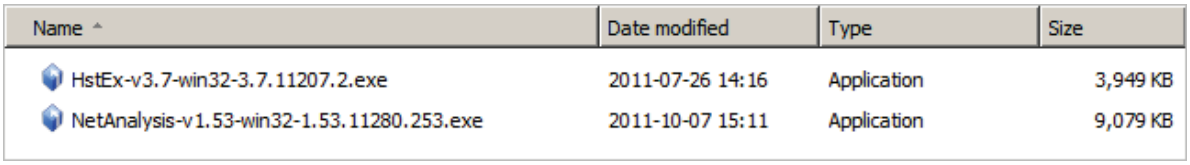


Figure 30

Good forensic practice dictates that you archive each release of HstEx that you use on a forensic case. This ensures that at any time in the future, you can install a specific version and replicate your results. When you run Setup, you will be prompted to select a language. This language selector is for the installation only and does not change the language used by NetAnalysis or HstEx (which is currently English).

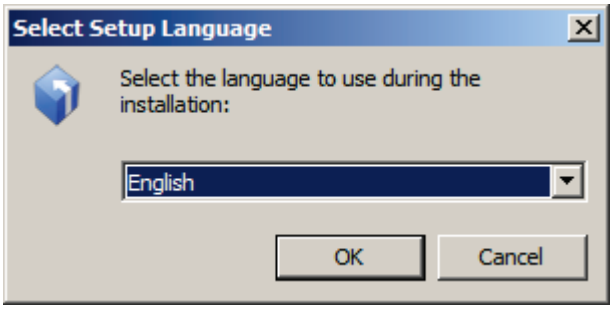


Figure 31

Select the appropriate language and click OK to launch the Setup Wizard (as shown in Figure 32).

Figure 32

End User Licence Agreement

The next screen displays the End User Licence Agreement. Please read this carefully. If you wish to review or print a copy of this agreement, it can be found in our knowledge base:

- *http://kb.digital-detective.co.uk/x/flUU*

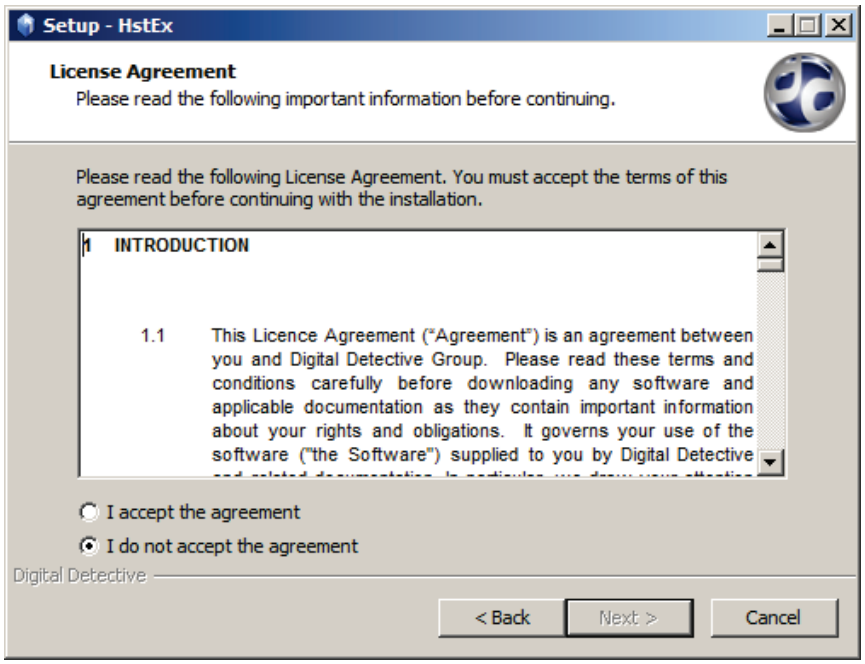


Figure 33

If you accept the agreement, please select the appropriate option and click Next. The next screen (Figure 34) prompts you to select a location in which to install HstEx. Please note this is a different location from where HstEx v1 - 2 was installed.

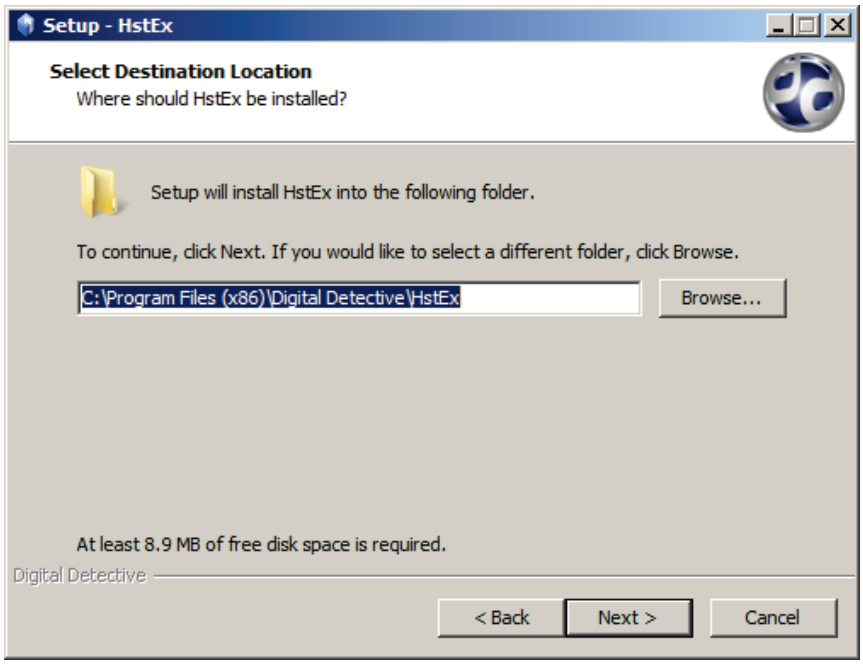


Figure 34

This next screen (Figure 35) allows you to select which components to install. There is no need to install the Licence Key Management Utility if you are using a USB Dongle Licence.

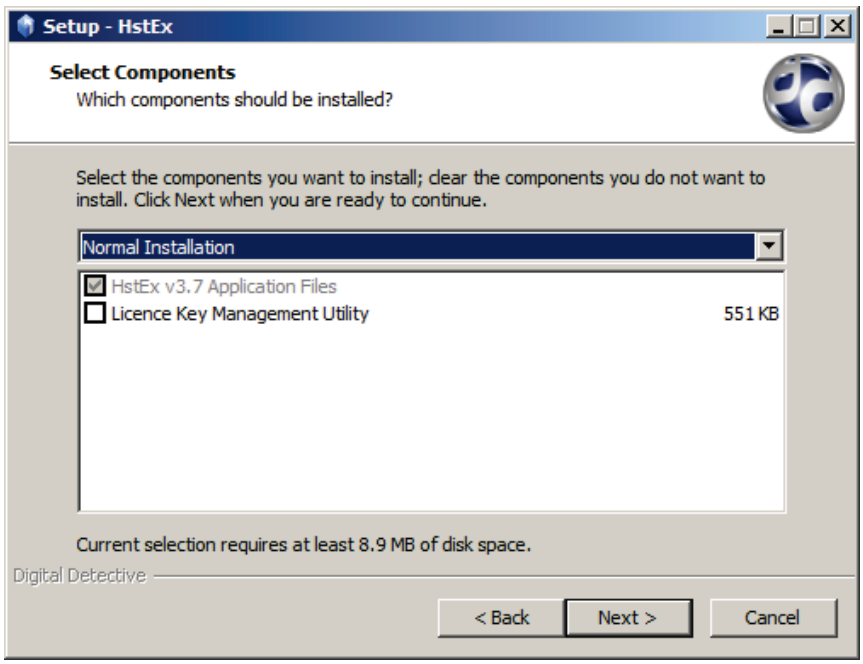


Figure 35

The next screen (Figure 36) shows the location of the Start Menu folder where the icons for the software will be placed. The default location for HstEx is in a folder called Digital Detective. You will find all our products in this location.

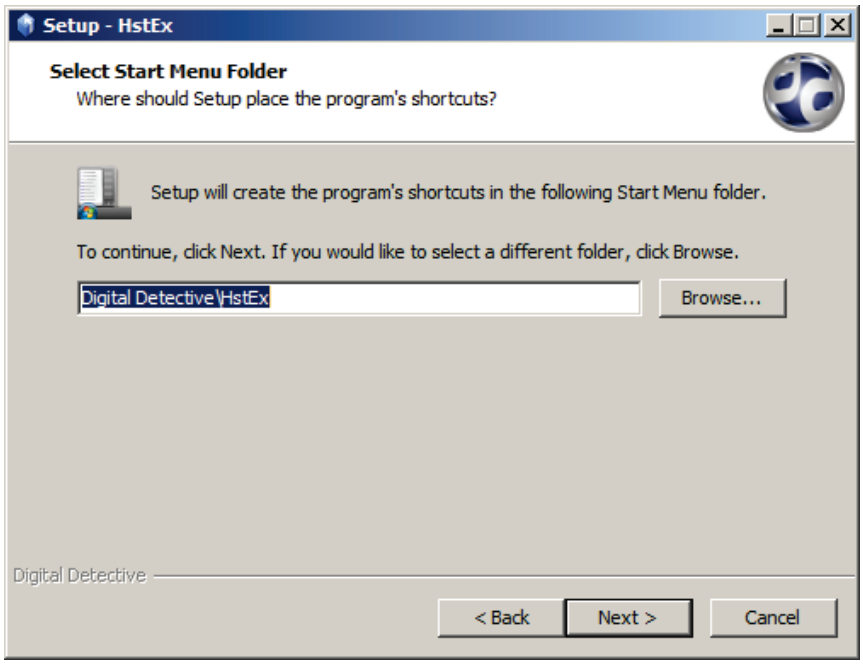


Figure 36

The next screen (Figure 37) shows additional tasks and gives you the option to create an icon on your Desktop.

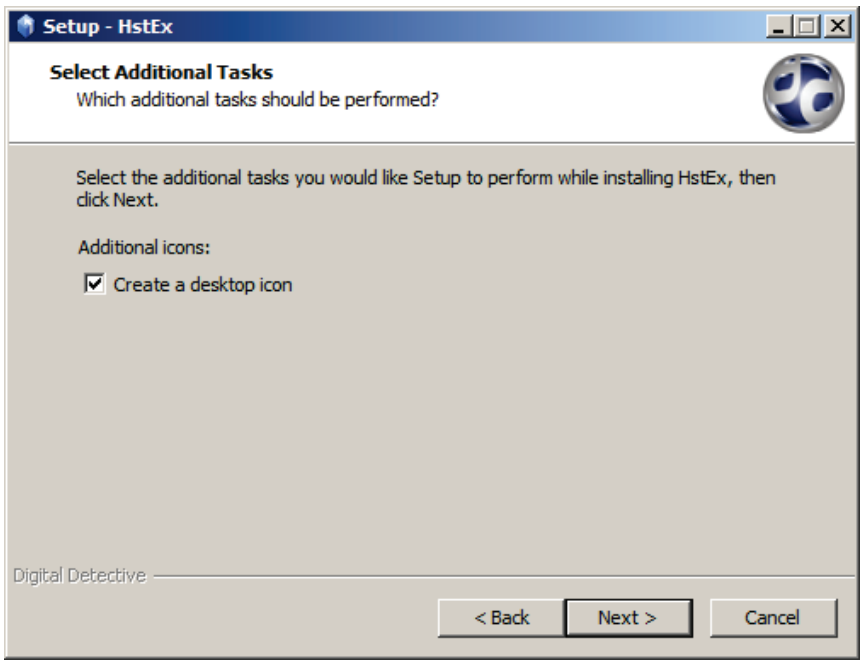


Figure 37

The next screen (Figure 38) shows a summary of the installation tasks prior to launching the installation process.

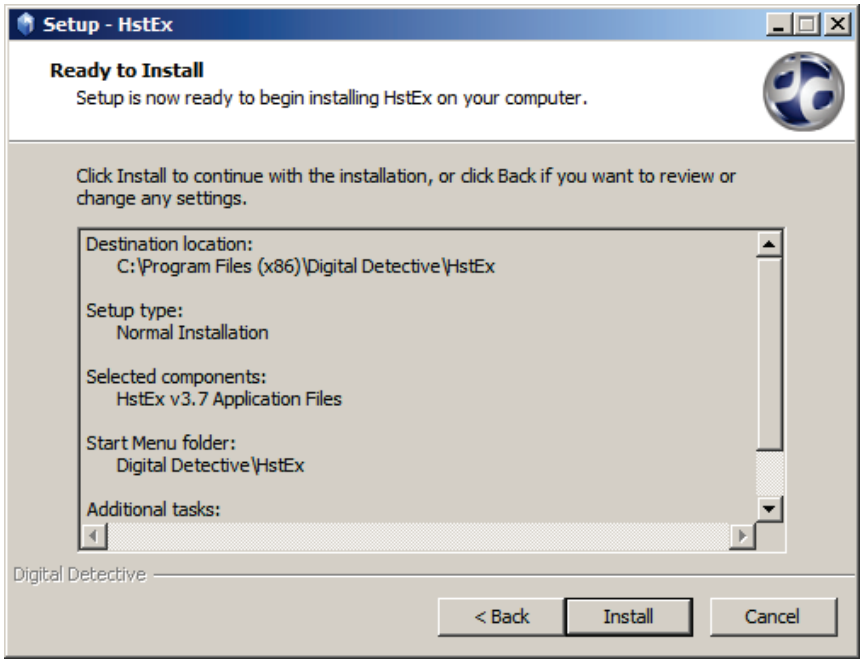


Figure 38

The next screen (Figure 39) shows important information in relation to installing a static Licence Key File or using a USB Dongle.

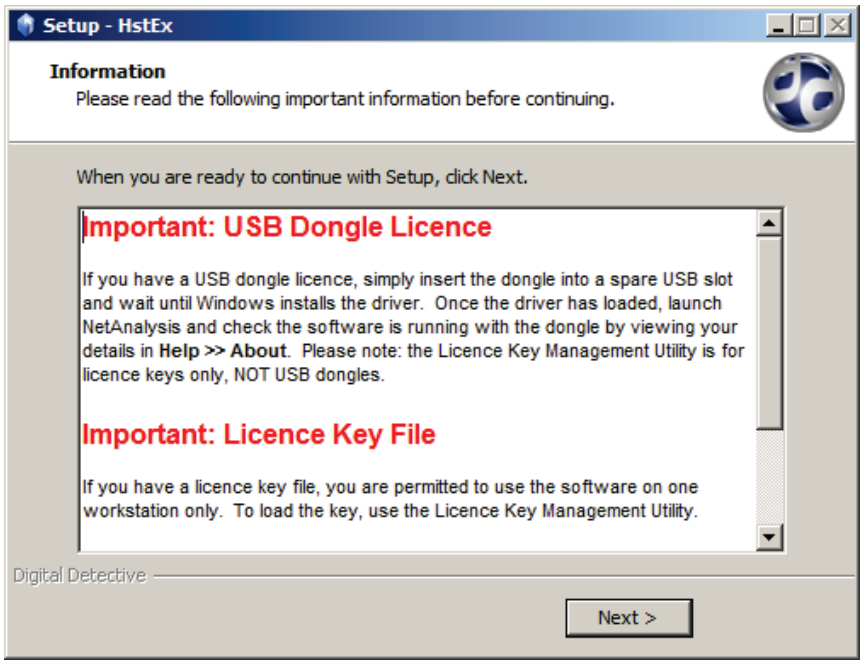


Figure 39

The final screen (Figure 40) shows that the HstEx Setup Wizard has completed. At this point, you may be asked to reboot your workstation. Please ensure this is done before you try and use HstEx.

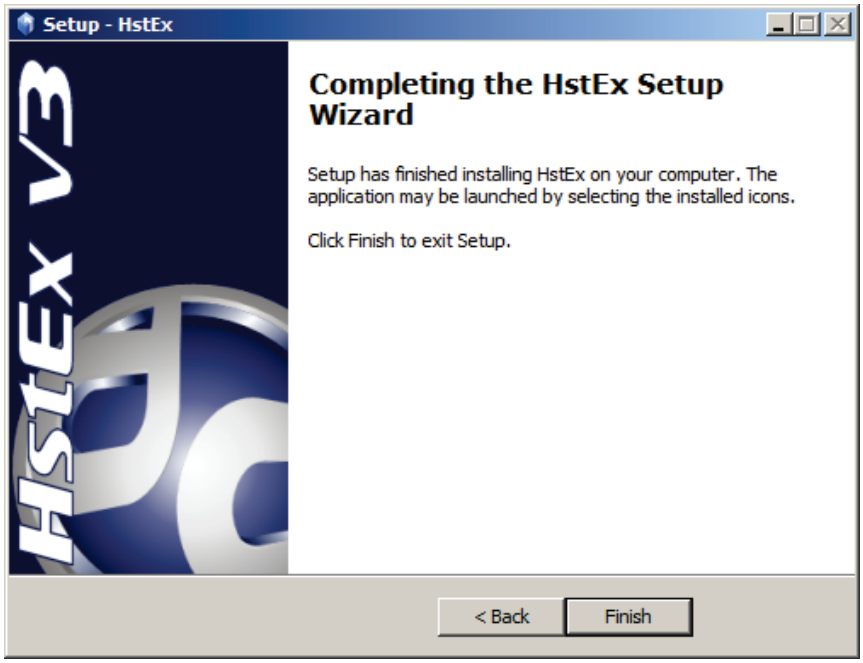


Figure 40

Default File Locations

The default installation folders for HstEx on 32 and 64 bit Windows are shown in Table 6 below.

Operating System	Path
Windows 32 bit	C:\Program Files\Digital Detective\HstEx\
Windows 64 bit	C:\Program Files (X86)\Digital Detective\HstEx\

Table 6

Installing a Licence Key File

Static Licence Key Files

NetAnalysis can use a licence key file to activate the full functionality of the software. The licence key file is normally sent to the end user by email and is contained within a zip archive.

The licence key file (netanalysis.lic) must be extracted from the zip archive and installed. In previous version of NetAnalysis, the licence key file was copied to the installation folder so that it was in the same physical location as the NetAnalysis.exe executable file. This is no longer the case in version 1.5x.

Do not copy the licence key file to the installation folder as was the procedure for v1.20 - 1.37. The licence key file is no longer accessed from this location. For information on installing a licence key file with NetAnalysis v1.20 - 1.37 and HstEx v1 - 2, see the following article:

http://kb.digital-detective.co.uk/x/OYAf

Licence Key Management Utility

In NetAnalysis v1.5x, you will use the Licence Key Management Utility to load the licence key. The benefits of using this utility are:

- It is much easier to install the licence key file;
- You can make back-up copies of your licence key file;
- You can review the status of your licence key and the licence summary information;
- You can activate NetAnalysis and HstEx at the same time.

Licence Key File Location

Although NetAnalysis versions from v1.5x and HstEx from v3.x use the Licence Key management Utility to load the licence for convenience, you may still manually copy the licence if you wish. The new licence locations are as follows. HstEx also shares the licence in these locations.

Operating System	Path
Windows 2K, XP	C:\Documents and Settings\All Users\Application Data\Digital Detective\NetAnalysis\Common
Windows Vista, 7	C:\ProgramData\Digital Detective\NetAnalysis\Common

Table 7

USB Hardware Dongles

Hardware Licence Dongles

The USB hardware licence dongle (as shown in Figure 41) is a small hardware device that plugs into a USB port on a host computer to provide licence information to our software.

Figure 41

Our dongles are based on an advanced microprocessor smart chip which has been certified by EAL4+ and ITSEC.

Installing and Using

The dongles register with the operating system as an HID (Human Interface Device). The generic HID drivers will be installed when the dongle is first inserted. As they require no external device driver during installation, this minimises the common technical issues which surround the use of hardware licences.

Once the HID device driver has been registered, simply inserting the USB dongle into a spare USB port prior to launching the application will allow the software to launch in a registered state.

You may have issues with the dongle being detected if you use a non-powered USB hub. In this situation, the USB device may not get the required voltage to operate correctly. Either use a powered USB hub or ensure you plug the dongle into a socket connected directly to the motherboard.

Please wait until the dongle LED stops flashing before you run any of our software otherwise the dongle may not be detected.

Upgrading Licences on a USB Dongle

Our USB dongles can be remotely updated and have the capability of storing licence information for numerous products and modules.

If you already own, or have purchased a licence update, new product or additional Blade modules, these updates can be added to an existing dongle.

To update your dongle, you will need three things:

- Valid Digital Detective USB Licence Dongle (Figure 41)
- Digital Detective Dongle Manager Software
- Valid Dongle Update File (*.DDUpd) for your specific dongle

Obtaining the Dongle Manager Software

To upgrade your dongle, we will email you with the latest download link for our Licence Manager as well as a Dongle Update File. This file can only be used once and will only upgrade the dongle it has been generated for.

Each dongle is uniquely identified by an electronic ID number (Dongle ID) which is hard coded into the device (cannot be changed) and a serial number which is etched onto the outside of the metal contacts.

The Licence Manager (as shown in Figure 42) can be used to review the licence information stored in the dongle and allows you to copy this information to the clipboard.

The software can also update the Dongle with a valid Dongle Update File (*.DDUpd). The Dongle Update file will be emailed to you as and when required (e.g. when additional modules or products are purchased).

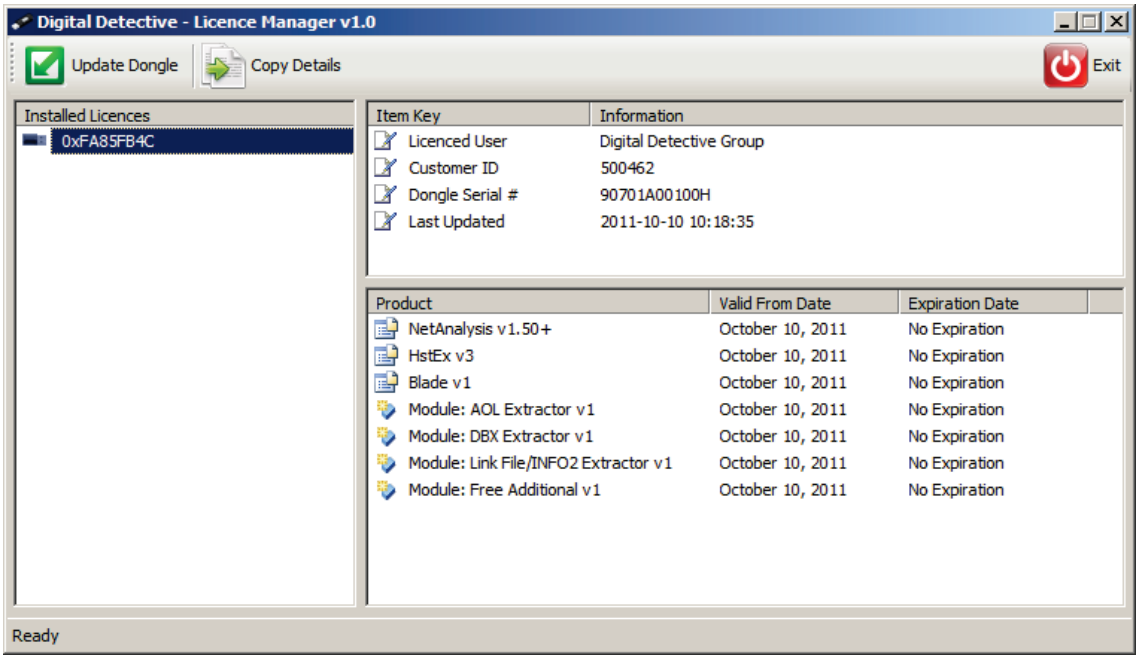


Figure 42

Once you have installed the software, please follow the instructions below to update the dongle. When updating the USB dongle, it is extremely important that the dongle is not removed from your system (or the system powered down) as this could result in the hardware being damaged.

Procedure for Updating a USB Dongle

To update the dongle, please follow the following instructions:

- Run the Licence Manager software
- Insert the USB dongle you wish to update
- Click on the USB Dongle ID in the Installed Licences list
- Make sure you have a corresponding update file (e.g. 0xFA85FB4C.DDUpd)

WARNING: It is extremely important that during the update process the dongle is not removed and that the system power remains on. If these instructions are not adhered to, there is a likelihood that the device will be permanently damaged!

Click on 'Update Dongle' and select the corresponding Update File (as shown in Figure 43). In this example, we are updating a dongle with the ID: 0xFA85FB4C.

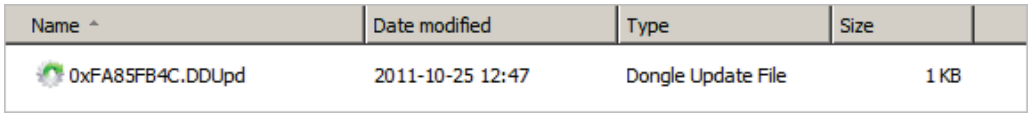


Figure 43

When you select the appropriate update file, you will see a warning message (Figure 44) asking you if you wish to continue and update the Dongle. Click 'Yes' if you wish to apply the update to your dongle.

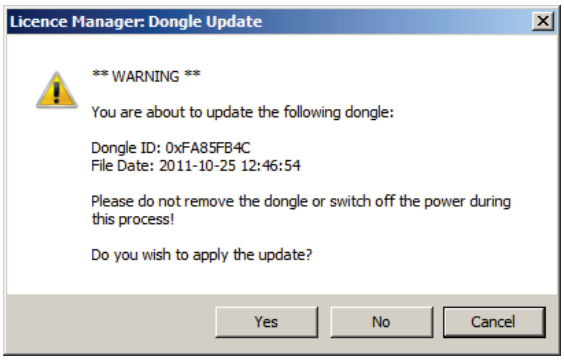


Figure 44

The Licence Manager will then update the licence information on the dongle and will display a message to show this has been successfully completed. The update process should take no longer than 5 seconds. Once the message has been displayed to inform you the update was successful, the Licence Manager will reload the dongle and display the new licence information.

You may now close the Licence Manager and remove the USB dongle if you wish.

Practice Files

Sample Data

To assist you in getting to know the NetAnalysis user interface, and to practise using the software in a safe learning environment, we have provided some sample data. Working through the examples will help you become familiar with using our software effectively within a forensic environment.

To access and download the sample data, please visit:

- *http://support.digital-detective.co.uk/2011-10-19-Data.zip*
- *http://support.digital-detective.co.uk/2011-10-19-Image.zip*

Case Scenario

On 19th October 2011, Victor BUSHELL, a resident of the United Kingdom, was arrested by HM Revenue and Customs at the Port of Dover in Kent whilst attempting to leave the country, bound for France.

He had in his possession a forged passport, a laptop computer and €20,000. It is believed BUSHELL is involved in the importation of illegal weapons into the United Kingdom.

His laptop has been imaged and is currently being examined. You have been tasked with reviewing his Internet browsing history. Everything you need for this case is available in the sample ZIP archive.

It has been established that the laptop computer was running Microsoft Windows 7 (64 bit). The suspect was using Microsoft Internet Explorer as a web browser.

File	Information
2011-10-19-Data.zip	This file contains the relevant exported files from the laptop computer. Contained within this zip archive, you will find files belonging to Internet Explorer, as well as registry hives.
2011-10-19-Image.zip	This file contains an EnCase® E01 evidence file of the seized laptop. The volume was formatted, prior to imaging, to demonstrate the data recovery capabilities of HstEx.

Table 8

NetAnalysis: A Guided Tour

NetAnalysis

To get the most from the software it is important to understand the user interface and know what each feature does. In this chapter, we will look at the various components of the user interface and understand how they work.

Main User Interface

This is the main NetAnalysis interface.

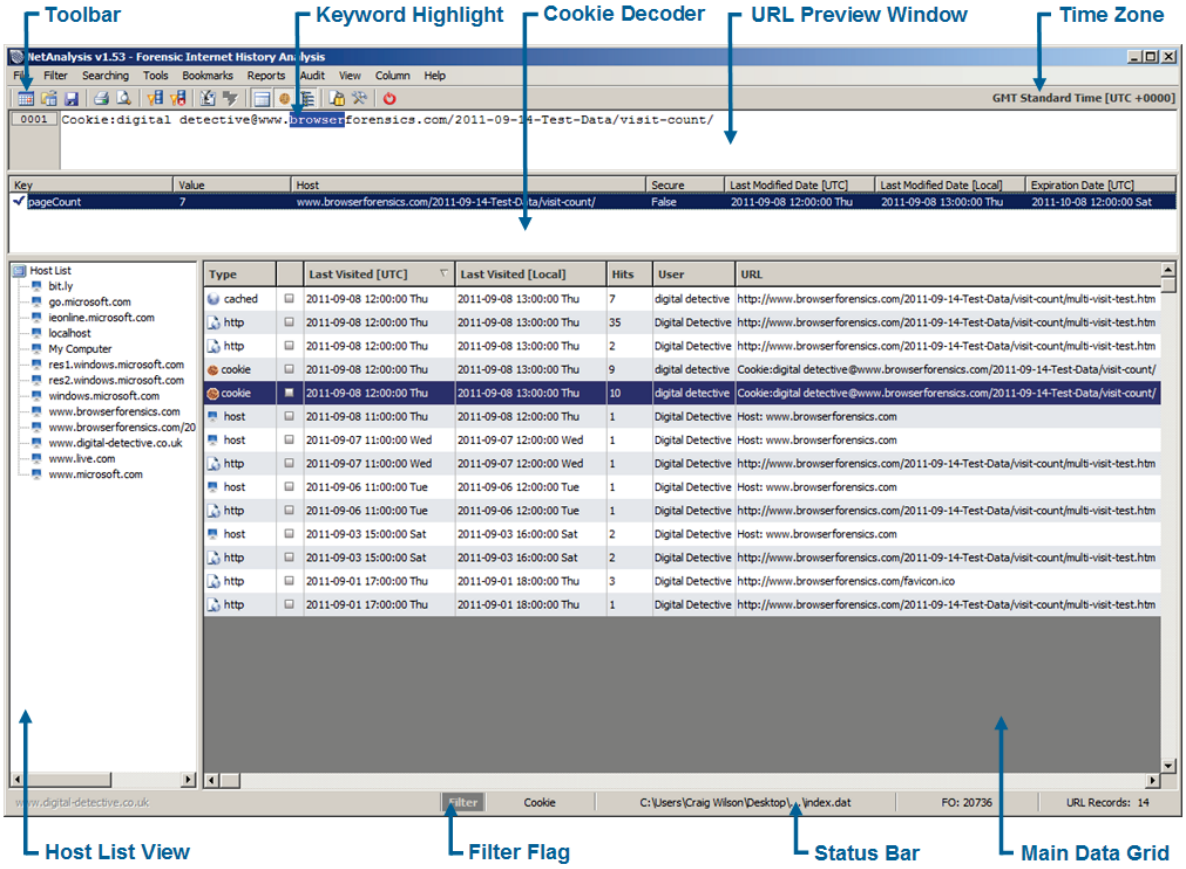


Figure 45

NetAnalysis has many features to assist with reviewing browser evidence such as full URL view, data decoding, keyword search highlighting and record bookmarking.

Main Toolbar

The toolbar contains a number of buttons for the more common functions. On the right hand side of the toolbar, the time zone Indicator shows the currently selected time zone for this investigation (for further information about time zone settings, please see Page 75).

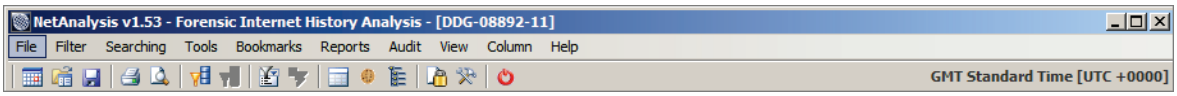


Figure 46

Table 9 holds a detailed explanation about the function of each toolbar button.

Button	Information
	Open History File This allows you to select individual (or multiple) source files for import. For example, if you wished to review the records from a single Microsoft Internet Explorer INDEX.DAT file, you can use this option to open and import the file. You can also use this button to import HstEx output files.
	Open Workspace This allows you to open previously saved NetAnalysis Workspace files for further review.
	Save Workspace This allows you to save the currently loaded data into a NetAnalysis Workspace file. You only have to press this once to save the workspace. Subsequent changes such as record book-marking or comments are automatically saved to the workspace. Workspace files contain a database which can be shared with other NetAnalysis users.
	Simple Print This will print the currently filtered records in a simple format containing the URL Type, Last Visited Date (Local Time), Username, Record Visit/Hit Count and URL. Additional report formats can be found on the Reports menu.
	Simple Print Preview This will show a preview window containing the simple print format as described above.

Button	Information
	Show Filter Form This is one of the most important buttons on the toolbar. This will launch the filter form which will allow you to quickly set a filter to identify the records in which you are interested. This should be one of your main methods for filtering and finding data. This function can be quickly accessed by pressing the keyboard shortcut key F8. The Filter Form is discussed in more detail later.
	Remove Filter This function will clear any selected SQL query or filter and return you to the full data set. This function can be quickly accessed by pressing the keyboard shortcut key F5. When this is pressed, the currently selected record will remain highlighted; this helps to prevent you from losing track of your position.
	Show Column Filter Bar This will activate the column filter bar at the top of the grid allowing you to enter filter keywords for any column. The filter can be activated by pressing the Execute Column Filter button (as shown below) or the ENTER key.
	Execute Column Filter This button will only be available when the Column Filter Bar is activated. Pressing the button will execute a filter query based on the keyword text entered into each column filter field. Wild cards can also be used in the query. For example, if you wanted to look at all activity between 07:00:00 and 07:59:59 hours on any particular day, you could enter 07:??:?? in the Last Visited column filter bar. You can also filter on multiple fields.
	Toggle URL Examination/Preview Window This button will toggle the URL Examination window above the main grid. When this is activated, the entire URL for the selected record can be easily viewed. This is particularly helpful for long URL records that cannot be easily viewed on the screen. This window will also highlight individual keywords contained within the URL when the records have been filtered via the Filter Form (activated by the keyboard shortcut F8 - see Show Filter Form above).
	Toggle Cookie Decoder This button will toggle the Cookie Decoder window above the main grid. When a cookie record is selected, if there is a corresponding cookie record available for decoding, it will be displayed in this window.

Button	Information
	Toggle Host List Window This will toggle the Host List window. Selecting this function will show each unique host in the workspace. This is a quick and easy function to examine which web sites have been visited by the suspect. If you click on any host within this window, it will filter the actual history records associated with this host.
	Show Audit Log This button will show a preview of the Audit Log which is maintained by NetAnalysis. The Audit Log contains information regarding the imported files and also metadata from HstEx source files (which may also contain further metadata from source evidence files such as that contained within EnCase® e01 images).
	Options This button activates the main Options window where NetAnalysis can be configured. The time zone extraction settings can also be accessed from here prior to importing any data.
	Exit NetAnalysis This button will exit the software. NetAnalysis will prompt the user if the Workspace has not been saved.

Table 9

Status Bar

The status bar contains some useful information in relation to the selected record, the number of records currently filtered in the workspace, as well as flag indicators for filtering and tagging. Figure 47 shows the status bar when a workspace is loaded. Table 10 holds a detailed explanation of the meaning of each panel.

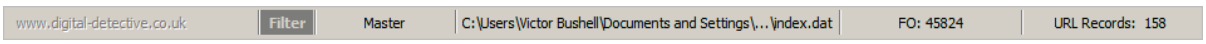
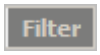
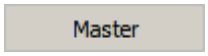
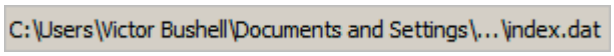
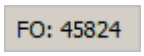


Figure 47

Status Bar Information
   This panel is a flag to show whether a TAG has been set on this record or not. This is the flag to indicate a TAG has been set on this record.

Status Bar Information

This panel is a flag to show whether a FILTER has been set on the current workspace or not. This is the flag for a FILTER which has been activated.

This panel reflects the Index Type field and will identify the type of record currently selected. In this case, the selected record is a Microsoft Internet Explorer 'Master' record.

This panel reflects the Source File field and will identify the origin of the original record. Used in conjunction with the Source Offset column, this information allows the forensic examiner to seek to the location of the source data in a secondary tool.

This panel reflects the Source Offset column and will identify the location of the record within the original data. This will either be a File Offset or Physical Sector (and Sector Offset) depending on the source type. This section is used in conjunction with the Source File field to identify the exact location from which the record was recovered. In a database or record based file where a specific file offset cannot be identified, this will show the record number or index.

This panel shows the total number of records currently filtered in the workspace.

Table 10

Column Headers

To fully understand the extracted data as presented by NetAnalysis, it is important to understand the type of data held in each column (or field). In this section, we will examine each column header and identify what type of data is stored in that field.

Type

The type field in history files reflects the HTTP scheme or protocol for the selected record. For cache and cookie records, the type is updated to indicate the type of entry (e.g. cache/cookie). For download and other files, the type is updated to indicate the type of entry. This allows the examiner to quickly differentiate between history, cache, cookie and other record types.

If NetAnalysis identifies corruption when processing a record during import, the type indicator will show “corrupt”. You are likely to see some corrupt or partial records from data recovered by HstEx.

Tag

The tag field is a user set field which indicates whether the record has been tagged by the forensic examiner. A tag can be set or unset at any point to assist with reviewing the data. There is also an option on the Searching menu to jump back and forth through the tagged records (Searching » Find Next Tagged Record [F2], and Searching » Find Previous Tagged Record [Shift+F2]).

Last Visited [UTC]

There are a number of different date/time fields in NetAnalysis. This particular field shows the last visit date/time in UTC (Universal Coordinated Time). Not all date/time fields are available for every browser type.

Last Visited [Local]

This field shows the local time for the last visit; however, this value is dependent on the accuracy of the time zone settings which must be set prior to importing any data. You must check the time zone settings for the suspect system to ensure the local time is accurate. This value is calculated from the UTC field as explained above.

The time zone settings must be set to the same as the suspect system and not the time zone of the forensic examiner's workstation (see Time Zone Configuration on Page 75 for further information). All local timestamps are presented as local from the perspective of the suspect system time zone locale.

Hits

The hits field represents the count of visits or hits and is not always present in a cache or history record (it is browser dependent). Further information regarding this field can be found in the Digital Detective Knowledge Base.

User

The user field is only present in Internet Explorer data, and on Windows NT based operating systems represents the user name of the account which was logged on.

This data is not always present in cache entries. The string data will sometimes be presented in a different case from the actual account username.

URL

The URL field represents the Uniform Resource Locator and is a string value which specifies where a known resource is located and the mechanism for retrieving it. If for whatever reason the URL is missing, the text '!< URL MISSING >!' will be placed in the field, as shown in Figure 48.

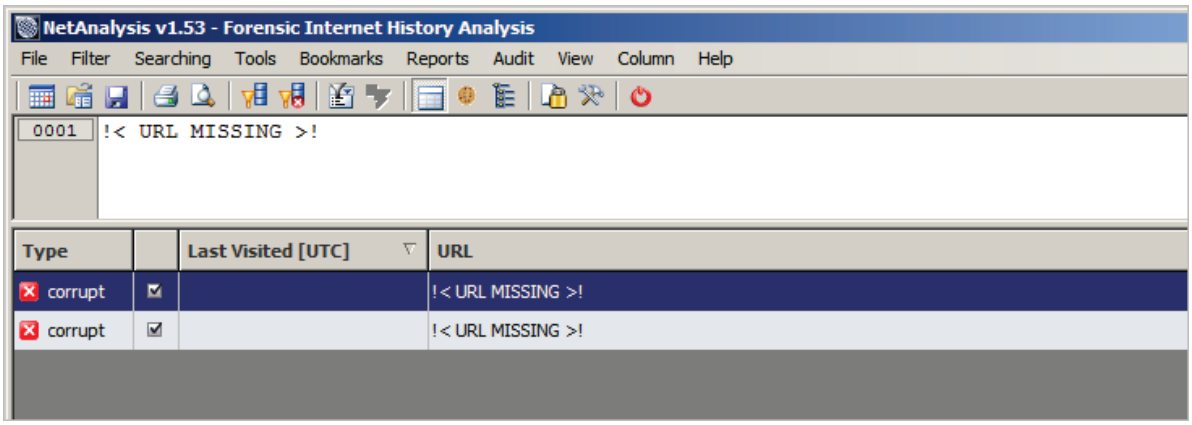


Figure 48

Host

The host field identifies the host that holds the resource. For example: www.example.com. The host is extracted from the URL.

Page Title

The page title field represents the title tag set by the web developer in the HTML code. The title can be seen in the browser title bar when the user visits a particular page. This information is usually present in History data.

Absolute Path

The absolute path field contains the path information that the server uses to resolve requests for information. Typically this is the path to the desired information on the server's file system; although it can also indicate the application or script the server must run to provide the information. The path information does not include the scheme, host name, or query portion of the URL.

Query

The query field contains any query information included in the URL. Query information is separated from the path information by a question mark (?) and continues to the end of the URL. The query information returned includes the leading question mark. An example query string can be seen in Table 11.

Example Query String
?fuseaction=user.viewprofile&friendid=9999999

Table 11

Fragment

The fragment field shows any text following a fragment marker (#) in the URL, including the fragment marker itself. Table 12 shows the full URL with a fragment marker string.

Example URL with Fragment Marker String	Fragment Marker String
http://www.contoso.com/index.htm#main	#main

Table 12

Port

The port field defines the protocol port used for contacting the server referenced in the URL.

Token

This field contains text data which relates to a URL token. Tokens can be used during an authentication process.

Logon User

This field can either contain information extracted from a URL, or from data saved to a sign-on database. When the field represents the value from a URL, it relates to the user name portion from the URL in the format: 'UserName:Password'. If the data relates to a user name from a sign-on database, the string will be encrypted. NetAnalysis does not support the decryption of sign-on user names at this time.

Logon Password

This field can either contain information extracted from a URL, or from data saved to a sign-on database. When the field represents the value from a URL, it relates to the password portion from the URL in the format: 'UserName:Password'. If the data relates to a password from a sign-on database, the string will be encrypted. NetAnalysis does not support the decryption of sign-on passwords at this time.

Redirect URL

URL redirection (also called URL forwarding) is a technique on the World Wide Web for making a web page available under many URLs. If a page is arrived at as a result of redirection (Internet Explorer will only show Server Side Redirects, i.e. where the server returns a 300 HTTP response code) this field shows where the browser was redirected to. The URL column will show where the browser was redirected from.

Feed URL

This field represents a URL to a valid RSS feed.

Referral URL

When a user clicks on a hyperlink within an HTML page, the web browser sends a request to the corresponding web server for the new page. As part of the request header, the browser also sends URL information relating to the page containing the link. This URL is called the referring URL.

The referrer field is very interesting from a forensic point of view as it shows the URL from which the visit originated. For example, Mozilla Firefox records this information for each record. It is therefore relatively easy to track the actions of a user from page to page.

Download Path

This field shows the path (relative to the local machine) where the user has selected to save a downloaded file.

Cache Folder

This field shows any sub-folders that may be present when identifying the location of a cached file. This field is used for Internet Explorer, Firefox v4+ and Opera v10.5+ cache.

Cache File

This field shows the name of the file containing a cached resource or object. In a download record, this field will show the name of the downloaded file.

Extension

This field shows the file extension of the cached (or downloaded) resource from the “Cache File” field. This column was added to make it easier for examiners to identify and filter particular file extensions.

Length

This field relates to the original length of a cached or downloaded item in bytes.

Exists

This field indicates whether a cached item exists in the recovered cache data. As the data is imported, the local cache path is identified and a test made to see if the resource exists. If it does, the item will be available for review or export.

If a cached item or object does not exist (or the record is not a cached item) the menu items relating to exporting the item (or rebuilding a page) will be disabled.

This field also indicates the existence of page content data in Google Chrome 'History Index' files.

We do not check for the existence of downloaded files as this data may not be present during the import of browser related files.

HTTP Response

This field holds the HTTP response data which has been collected by the browser during the download of a resource object. Different browsers store different portions of the HTTP response and not all fields may be present.

Cache Entry Type Flag

This field is only used for Microsoft Internet Explorer and shows the flags that were set for a particular cached entry. They can be: Normal, Cookie, History, Edited, TrackOffline, TrackOnline, Sticky and Sparse.

Content Type

This field shows the cached object MIME type.

Content Length

This field shows the length of the cached object, in bytes, and is read from the HTTP response object. With a download record, this field reflects the length of the downloaded data.

Content Encoding

This field shows the HTTP content encoding scheme. This is covered in *Section 14 of RFC 2616* which covers Header Field Definitions.

ActiveBias

This field is only used for Microsoft Internet Explorer and relates to the time zone active bias at the time the visit was made. In the Daily INDEX.DAT file, there are two dates stored, one in local time

and one in UTC. Examination of these dates can show the offset from UTC. As NetAnalysis imports Internet Explorer data, it checks the bias difference between the Last Visited UTC/Local times and adds it to this column. NetAnalysis can also detect when the active bias parameters are outside the import time settings and will flag this issue to the examiner in the summary screen shown when the data has finished being imported.

Date First Visited [UTC]

This field shows the first visit to the URL. This field is only available with certain browser data types.

Date Expiration [UTC]

This field shows the expiration date for a cached object. HTTP supports caching so that content can be stored locally by the browser and reused when required. Of course, some types of data such as stock prices and weather forecasts are frequently changed and it is important that the browser does not display stale versions of these resources.

Browser caching is controlled by the use of the Cache-Control, Last-Modified and Expires response headers.

Date Last Modified [UTC]

This field shows the last modified date for a cached object. As with the “Date Expiration” field above, the web server can return a Last-Modified date as part of the HTTP response headers.

Date Index Created [UTC]

This field is used only in Microsoft Internet Explorer and is recovered from Weekly INDEX.DAT records. It reflects the date/time value when the INDEX.DAT file was created.

Date Added [UTC]

This field shows the date a cached object was added to the cache.

Date Last Synch [UTC]

This field shows the date a cached object was last synchronised.

Source File

This field shows the full path of the source file from which the record was recovered. If the source is a HstEx file, this field will show the original source that HstEx recovered from (e.g. an e01 image or physical device).

Source Offset

This field shows where the data was found within the source file. The offset can be displayed in a number of different formats depending on the source type. If the source is a physical device or an image representing a physical device, it will show the Physical Sector and Sector Offset (e.g. PS: 9058032 SO:384). If the source is file based, such as a binary dump, it will show the File Offset of the data from the start of the file (e.g. FO: 483273123). It does not always make sense to identify the exact location of data within a file by an offset; for example, if the data is recovered from a database it would make sense to show the database record index. Some other file types (e.g. Apple Safari binary PLIST) store the record data in different locations within the file, and the file offset will not assist in validating the recovered data. In these cases, we provide the record number or record Index. This is displayed as either an Index or ID.

Index Type

This field identifies the type of record. For example the record may be one of the following: History, Cookie, Cache, Download, etc.

Browser Version

This field represents any version information which has been identified during the extraction process. For example, many cache entries store a version number which can help identify the original browser version.

IE Type

This field relates to Internet Explorer only and reflects the type of record in the INDEX.DAT file. Possible entries include: URL, REDR and LEAK. Table 13 explains the purpose of each type.

Type	Meaning
URL	This is a standard URL record for Internet Explorer which is not a redirect or a LEAK.
REDR	This type of record relates to a Server Side Redirect. This record contains a string relating to the URL which caused the redirection. If the data is still available, NetAnalysis can identify the record containing the date/time information and URL the browser was redirected to.
LEAK	This type of record relates to a cache or cookie item that Microsoft Internet Explorer was unsuccessful in removing. This may have been due to the file being locked or in use when the attempt was made. This record would have originally been a URL record that had subsequently been updated to LEAK status to indicate it could safely be removed at a later stage. LEAK records are often incomplete and may not show the full original URL.

Table 13

Status

The status field contains further information relating to a particular record, which may be available from the original file, and has no corresponding NetAnalysis workspace column. It can also display information such as flagging partially corrupt records.

Bookmark

The bookmark field is set by the forensic examiner and contains a string field that can be used to identify or describe a record. The bookmark string appears in the Advanced Report and is commonly used to annotate particular records when they are of evidential value to your case.

When a record of interest is found, the bookmarking function can be used to highlight and comment each individual record. Any bookmarked records will show a bookmark icon before the start of the URL. In Figure 49, the bottom record has been bookmarked.

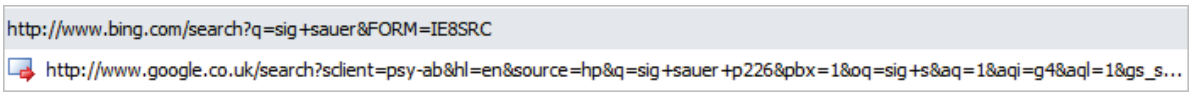


Figure 49

URN

This field represents a Unique Reference Number and is allocated by NetAnalysis during the import process. It can be used to easily identify a particular entry in a workspace. When a cached item is exported or a cached page rebuilt, this Unique Reference Number is used to reference the exported file. Any exported resource will have the same URN as its corresponding record in the NetAnalysis Workspace. If you order the records in the workspace by URN, you will see the order in which they were imported.

URL Examination Window

The URL examination window can be activated by clicking on the URL Examination Window button on the toolbar or from the following menu: View » URL Examination Window.

When this is activated, the entire URL for the selected record can be easily viewed. This is particularly helpful for long URL records that cannot be easily viewed in the main grid. This window will also highlight individual keywords contained within the URL when the records have been filtered via the Filter Form (activated by the keyboard shortcut F8 - see Show Filter Form in Table 9).

Figure 50 shows the URL examination window with the identified keyword highlighted in blue. Keyword highlighting makes it easy to quickly identify relevant search hits when trawling through a large workspace of possible evidence.

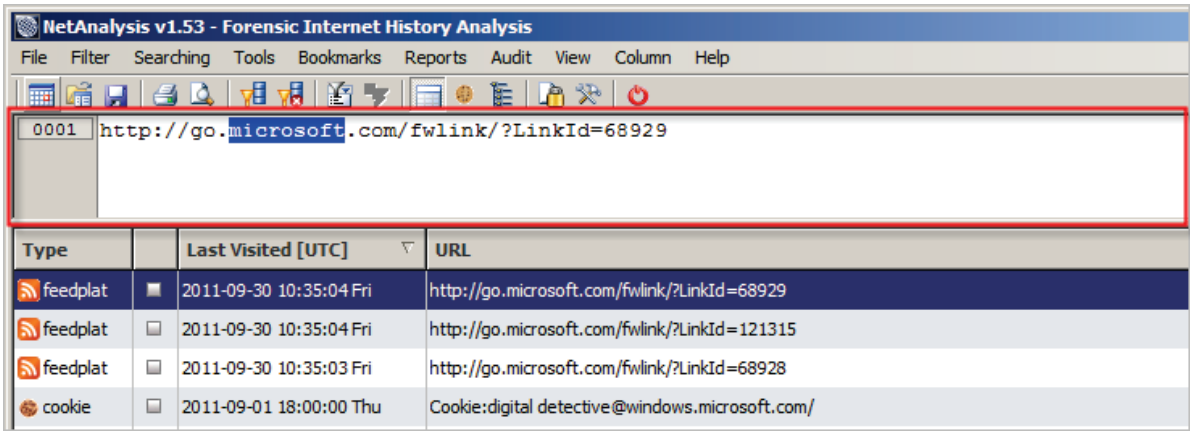


Figure 50

Cookie Decoder

NetAnalysis has its own built-in cookie decoder. It can be activated by clicking on the Cookie Decoder button on the toolbar or from the following menu: View » Cookie Decoder.

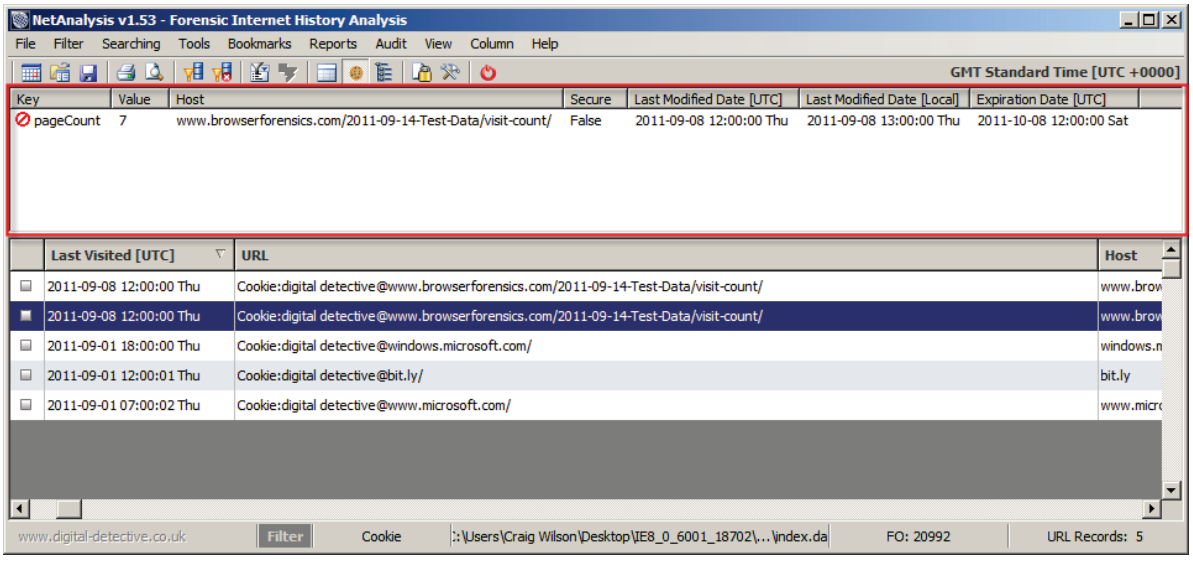


Figure 51

When a cookie record is selected, if there is corresponding cookie data available, NetAnalysis will load it into the Cookie Decoder grid, as shown in Figure 51.

Each cookie record has an icon to the left of the record to indicate whether the cookie has expired or not. This is an indicator only field and is measured against the clock on the forensic workstation. In this example, the cookie has expired.

The Cookie Decoder column fields are explained as follows:

Key

Cookie data is stored as key/value pairs. Microsoft Internet Explorer cookies are stored within a cookie text file and can hold multiple key/value pairs. This column shows the 'key' portion.

Value

This column holds the value part of a key/value pair.

Host

This field contains the Host (and path information) for the selected cookie record.

Secure

Cookies can be transported in a Secure or Non-Secure fashion. Once they are stored on the disk, the data is in plain text. However, this does not prevent developers from encrypting the individual key/value pairs. Secure cookies can only be sent over HTTPS (SSL). Non-Secure cookies can be sent over HTTPS or regular HTTP. The title of secure is somewhat misleading. It only provides transport security and reflects the method of transport, not the method of storage.

Last Modified Date [UTC]

This field shows the last modified date for a cookie object in UTC. This data is extracted from the cookie record.

Last Modified Date [Local]

This field shows the last modified date for a cookie object in Local Time. This data is extracted from the cookie record and reflects the calculation of Local time from the UTC value in accordance to the time zone settings in NetAnalysis.

Expiration Date [UTC]

This field shows the expiration date for a cookie object in UTC.

Host List View

The Host List window appears to the left of the main examination grid when activated (see Figure 52). Selecting this function will show each unique host in the workspace. It can be activated by clicking on the Host List button on the toolbar or from the following menu: View » Host List View - All.

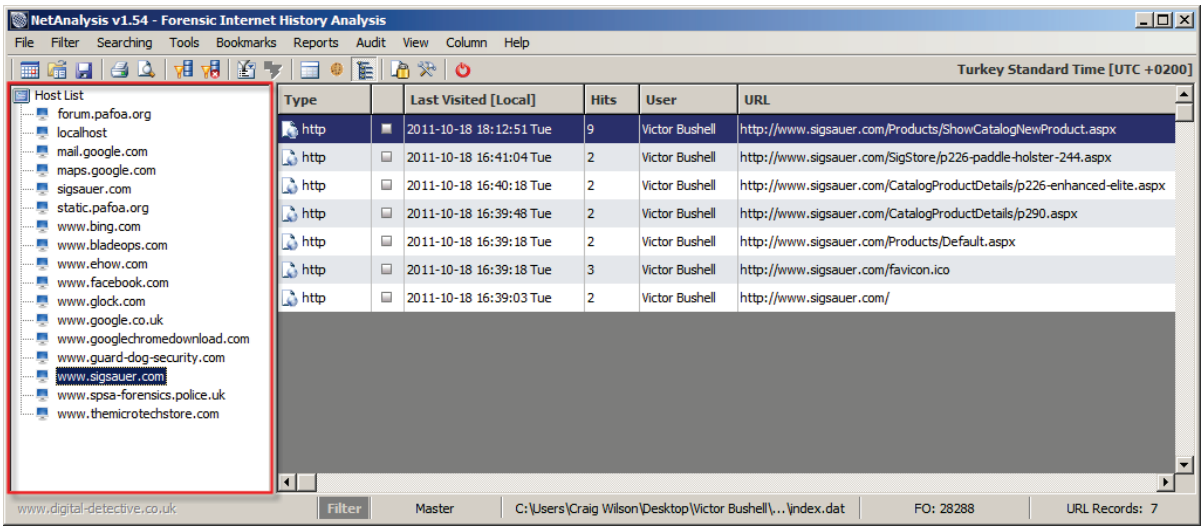


Figure 52

If you click on any of the host entries, the grid will filter to only show the records for that host. There is also a further menu option: View » Host List View - History Only. This option can be used when examining Microsoft Internet Explorer history and will show only the unique 'Host' records from Daily and Weekly entries.

Decode URL

Many Internet URL records, on first examination, are difficult to interpret. This is either due to the length of the data, or the use of encoding. The 'decode' function performs two actions:

- Decodes and replaces any standard URL encoding
- Splits the Query String into Name/Value pairs

To access the decoding function and display the decoded URL (as shown in Figure 53), right click on the record you wish to decode and select Decode URL. The query name/value pairs can also be seen in this example.

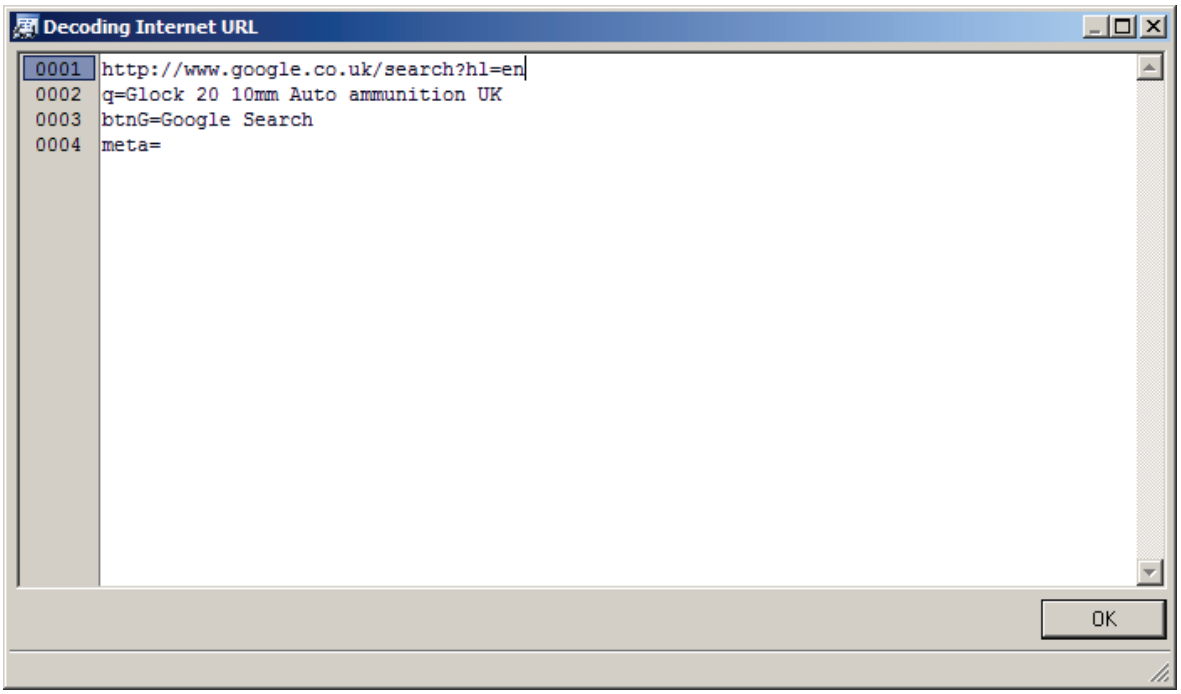


Figure 53

Record Bookmark

The bookmark field is set by the forensic examiner and contains a string which can be used to identify or describe an individual record.

The bookmark string appears in the Advanced Evidence Report and is commonly used to annotate particular records when they are of evidential value to your case. The Record Bookmark window (as shown in Figure 54), can be activated by any of the following methods when the corresponding record is selected:

- Press the Enter Key;
- Right click and select Add/Edit Bookmark;
- Select Bookmark » Add/Edit Bookmark from the main menu.

In the text box at the bottom of the window, the forensic examiner can enter a free text description for the URL.

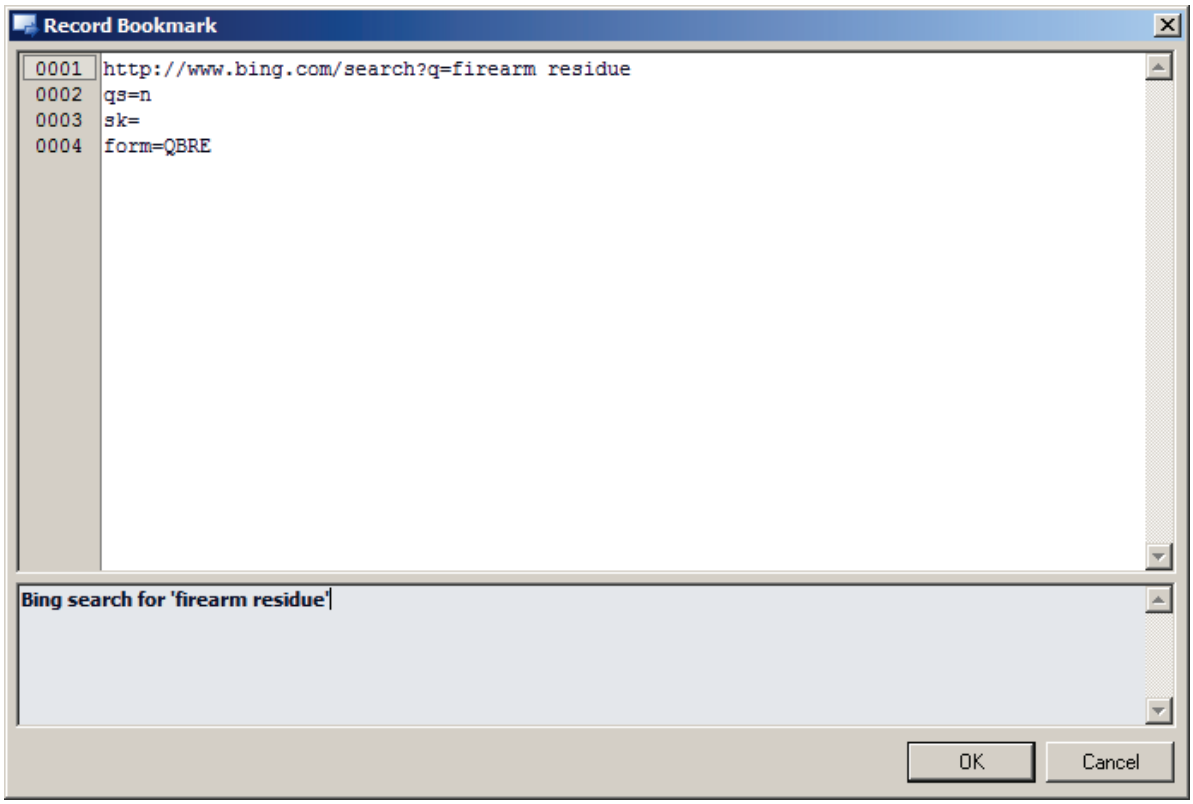


Figure 54

When the item has been bookmarked, the string text will appear in the bookmark column, as well as displaying a bookmark icon to the left of the URL (as shown in Figure 55).

Figure 55

Audit Log

During the process of extracting Internet history, NetAnalysis keeps an audit log that holds information such as who the software is licensed to, the date/time the analysis commenced, the Investigator, the time zone settings and the version of NetAnalysis used. The audit log can be saved as a separate PDF file if required.

The audit log also records the path and name of every file extracted. As a further check, NetAnalysis will also record the apparent time zone settings when it examines a Daily INDEX.DAT file. It is not unusual for the user of a suspect system to have the time zone set incorrectly, or to change the time zone settings at various times during the use of the system.

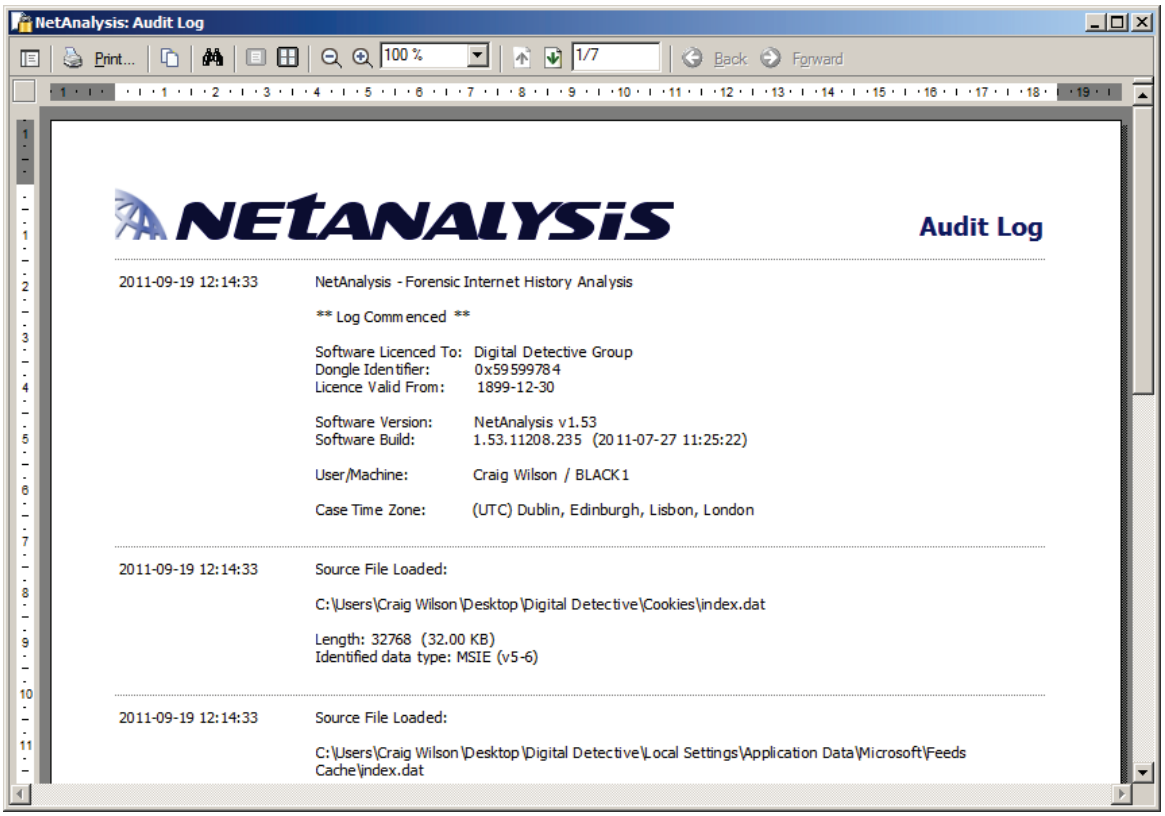


Figure 56

Column Filter Bar

In some cases, you might want to filter the underlying workspace by limiting the number of items in a given field or fields. By using the Column Filter Bar, and entering the filter text appropriately, you can reduce the number of records displayed. When the Column Filter Bar is activated, a blank row with a grey separator line appears directly above the uppermost data row in the grid (as shown in Figure 57).

It can be activated by clicking on the Column Filter Bar button on the toolbar or from the following menu: View » Column Filter Bar. To activate a filter, enter the filter text in the box immediately below the corresponding column and click the Execute Filter Bar button on the toolbar (or press the Enter key). For Boolean fields, enter 1 for true and 0 for false.

Type		Last Visited [UTC]	Last Visited [Local]	Hits	User	URL
						Glock
http		2011-10-19 08:46:59 Wed	2011-10-19 11:46:59 Wed	20	Victor Bushell	http://www.glock.com/english/glock17.htm
http		2011-10-18 13:43:24 Tue	2011-10-18 16:43:24 Tue	10	Victor Bushell	http://www.glock.com/english/navi_pistols_05.htm
cached		2011-10-18 13:43:23 Tue	2011-10-18 16:43:23 Tue	2	victor bushell	http://www.glock.com/images/glock_magazines.gif
cached		2011-10-18 13:43:23 Tue	2011-10-18 16:43:23 Tue	3	victor bushell	http://www.glock.com/images/glock_navigation_11.jpg
cached		2011-10-18 13:43:23 Tue	2011-10-18 16:43:23 Tue	3	victor bushell	http://www.glock.com/images/glock_navigation_10.jpg

Figure 57

Results Window

At the conclusion of an operation such as importing, exporting or web-page rebuilding, NetAnalysis will display a results window (as shown in Figure 58).

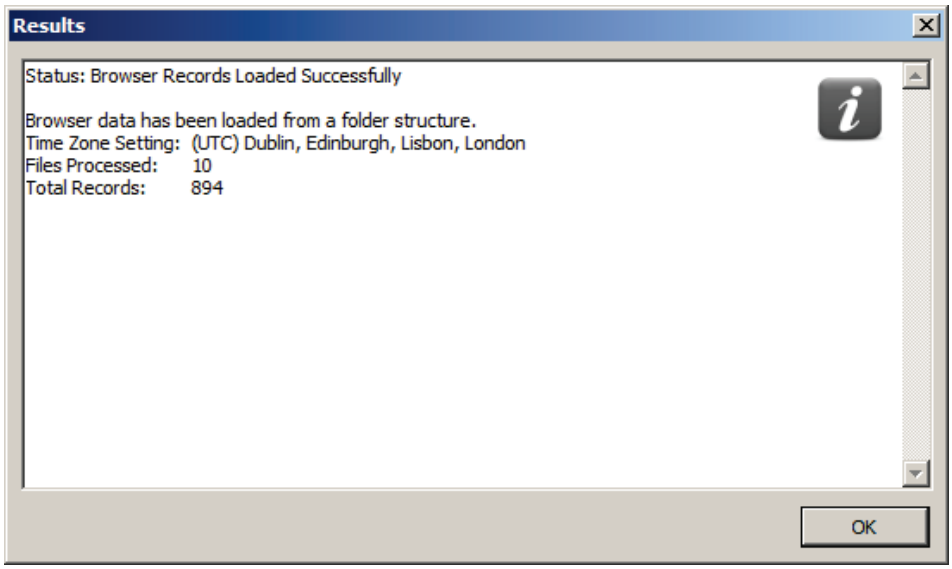


Figure 58

Configuring NetAnalysis

Before You Start

If this is a new (or first time) installation of NetAnalysis, it is recommended that you take some time to configure the software prior to using it live on a case. The Options window can be activated from the Options toolbar button, or from the menu: Tools » Options.

Import Settings: Time Zone

This page (as shown in Figure 59) allows the forensic examiner to set the time zone of the suspect system prior to importing any data. You must ensure you establish the time zone settings for your suspect system (see the chapter relating to Time Zone Configuration on Page 75) before you import any data into NetAnalysis.

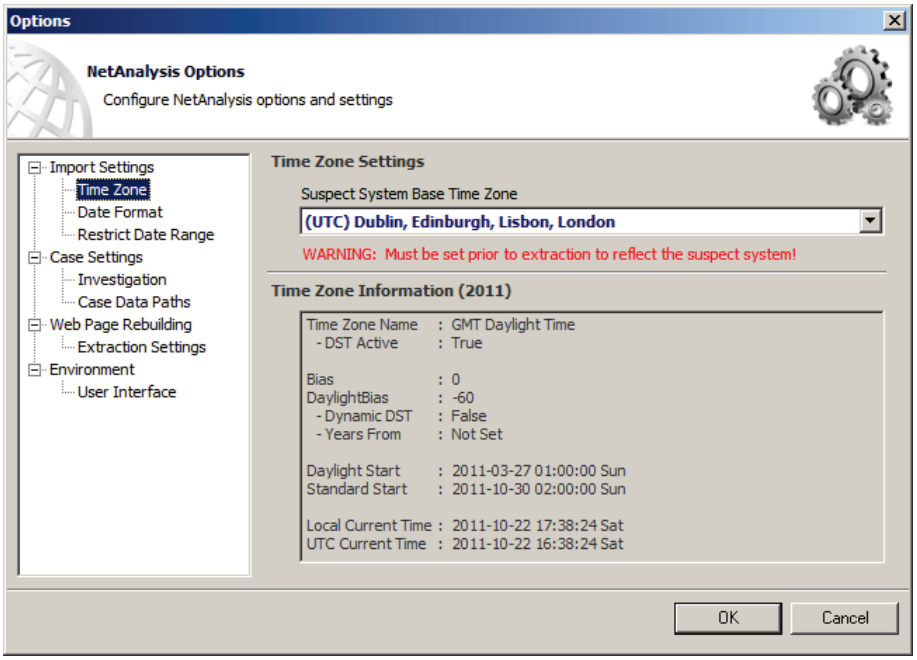


Figure 59

Once the time zone has been set for a case, it is saved with the workspace file and cannot be changed. This is to ensure that mistakes cannot be made by inadvertently adding further data once the time zone has been altered.

Import Settings: Date Format

This page (as shown in Figure 60) allows the forensic examiner to set the default date/time format. The default format will be initially read in from the workstation the software is installed on, but can be changed at any time.

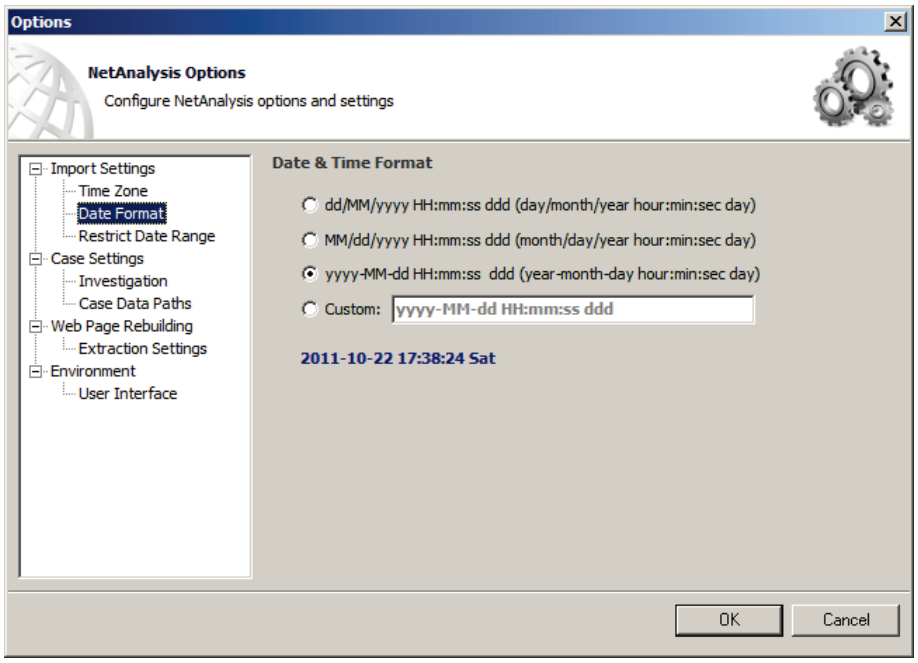


Figure 60

Import Settings: Restrict Date Range

This page (as shown in Figure 61) allows the forensic examiner to set a date/time restriction for the data you import. This option is disabled by default. The date restriction is tested during import against the Last Visited [UTC] field.

This option is particularly useful for the following scenarios:

- You have been given a mandate to only examine data within a specified date/time range (such as when directed by a Judge or within the parameters of a search warrant);
- You have recovered a large amount of browser related records but are only interested in a specific date range when an offence or incident occurred;

When this option is active, NetAnalysis will warn the user prior to importing any data. This option can be activated or deactivated at any time.

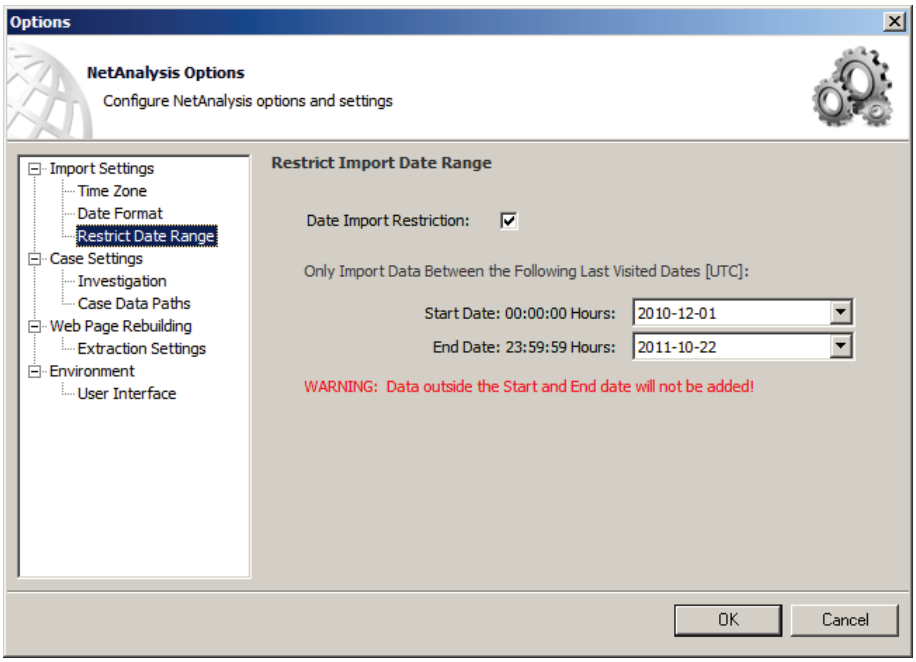


Figure 61

Case Settings: Investigation

This page (as shown in Figure 62) is only available once data has been imported into a workspace. It allows the forensic examiner to save case related information for their investigation. Some of this information is displayed in the printed reports. The forensic examiner will be prompted to complete this information prior to printing a report or exporting data (such as rebuilt web-pages).

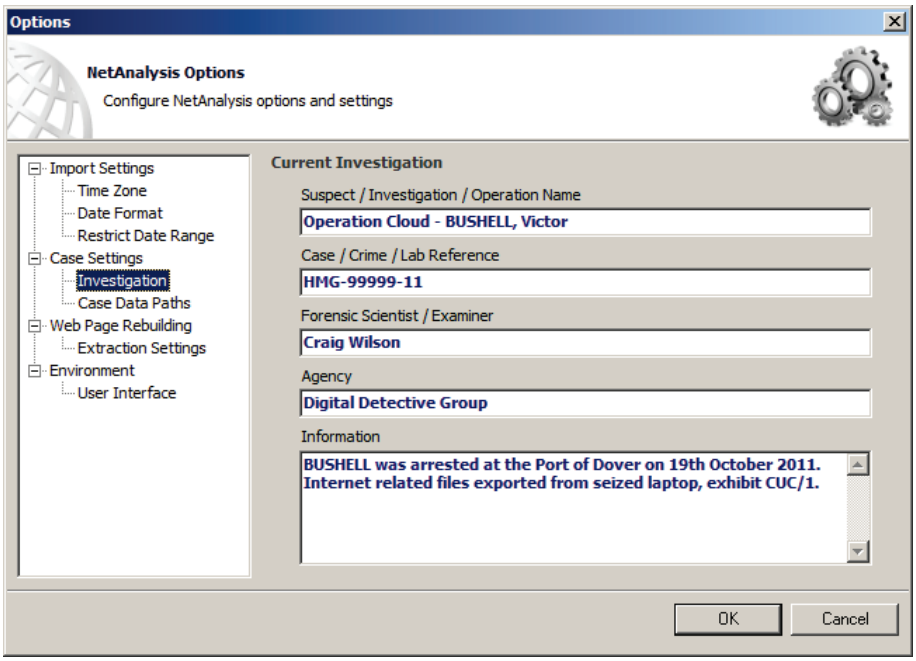


Figure 62

Case Settings: Case Data Paths

This page (as shown in Figure 63) is only available once data has been imported into a workspace. It allows the forensic examiner to set the export folder.

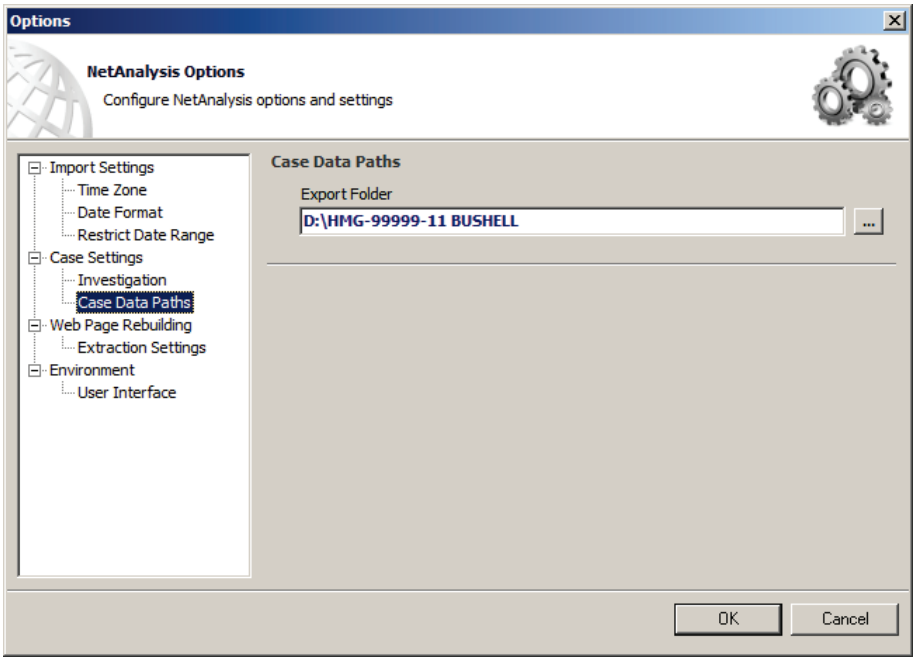


Figure 63

The export folder is used to hold exported objects such as:

- Exported Cache Objects;
- Rebuilt Web-Pages;
- Page Rebuilding Audit Logs.

Web Page Rebuilding: Extraction Settings

This page (as shown in Figure 64) allows the forensic examiner to set the parameters used in the rebuilding of web-pages and the export of cached objects (such as JPEG images).

Option	Meaning
Group Output Files by Extension	This option creates a folder for each file type stored in the cache (by extension) and when files are extracted they are copied to the corresponding folder.
Use Default File Viewer	This option sets whether to use the operating system default HTML viewer when viewing rebuilt web pages.

Table 14

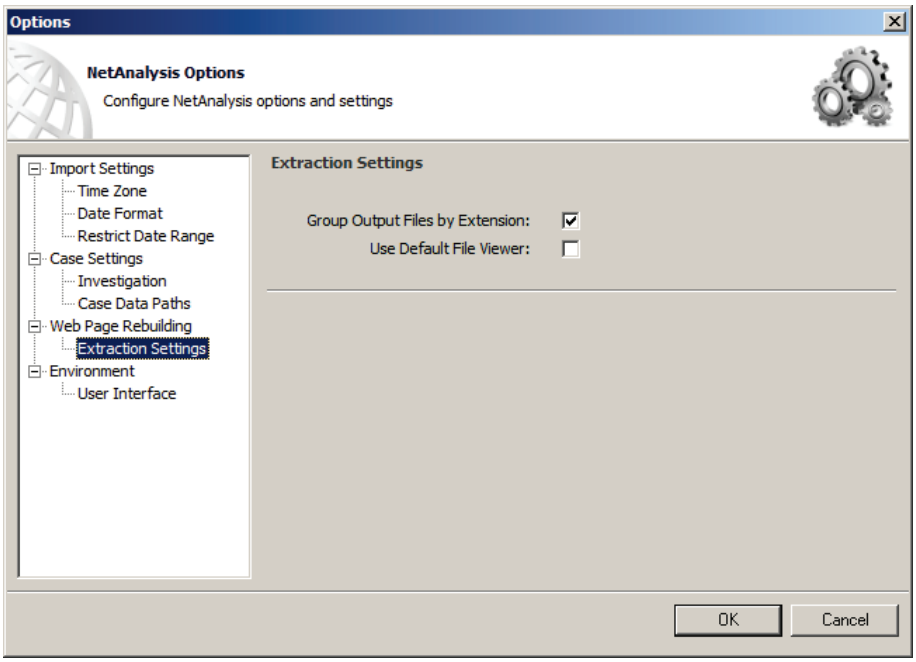


Figure 64

Environment: User Interface

This page (as shown in Figure 65) allows the forensic examiner to change some of the default settings for the user interface.

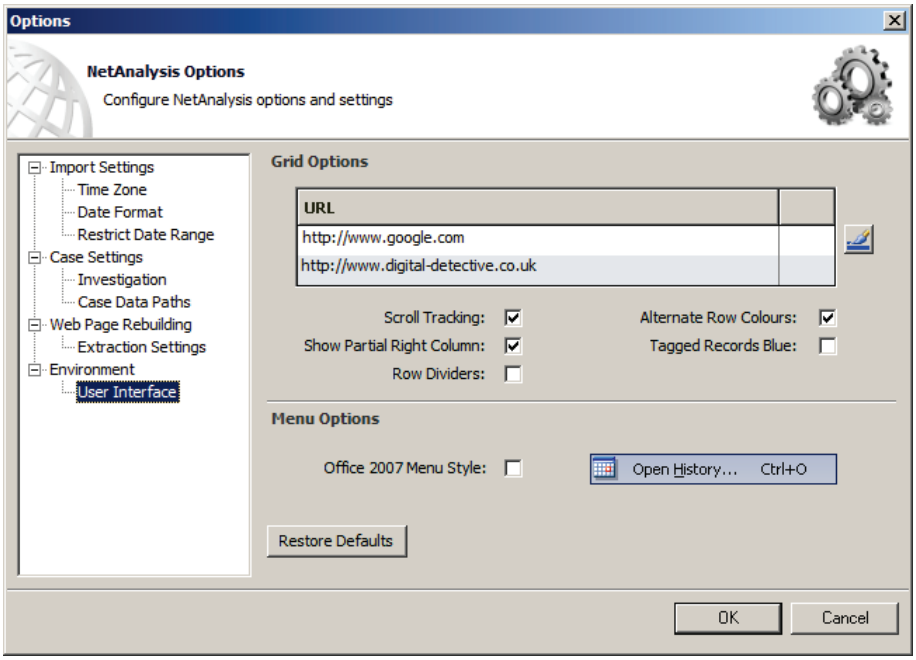


Figure 65

Time Zone Configuration

Introduction

In a forensic examination, establishing the time zone from the suspect system is one of the first tasks for a forensic examiner. If this information is not established at an early stage and taken into account, then the validity of all date/time values may be brought into question due to the way operating systems and browser applications store date/time information.

Date/Time Values

Operating systems and browser applications store date/time information in different ways using a variety of timestamp formats. Many timestamps are stored in UTC, and then converted to local time when presented to the user, and some are stored in local time. It is therefore vital to establish the correct time zone setting for the system to correctly convert these timestamps.

Universal Coordinated Time

Coordinated Universal Time (UTC) is the international standard upon which civil time is based and by which the world regulates time.

UTC is based upon UT1, which is the time determined by the rotation of the Earth. In accordance with international agreement, UTC and UT1 are not permitted to differ by more than 0.9 of a second. When it appears that the difference is approaching this limit, a one second change is introduced to bring the two back into alignment. On average, this occurs once every 12 - 18 months. Since the 1st January 1972, there have been 24 positive leap second adjustments.

UTC is the time standard used for many Internet and World Wide Web protocols. The Network Time Protocol (NTP) is designed to synchronise clocks and computers over the Internet and encodes time using the UTC system. It is widely used as it avoids confusion with time zones and daylight saving changes.

Each local time is represented as an offset from UTC, with some zones making adjustments during the year for daylight saving.

Greenwich Mean Time is a widely used historical term, however, due to ambiguity, its use is no longer recommended in technical contexts.

Daylight Saving and Standard Time

UTC does not change with a change of seasons; however, local time or civil time may change if a time zone jurisdiction observes Daylight Saving Time or summer time. For example, UTC is 5 hours ahead of local time on the east coast of the United States during the winter but 4 hours ahead during the summer. Not all time zones observe daylight saving.

To deal with the numerous time zone changes throughout the world, Microsoft periodically release a time zone update [2] to accommodate Daylight Saving Time (DST) changes in several countries.

How NetAnalysis deals with Time Zones

NetAnalysis provides the forensic examiner with the necessary tools to automatically convert UTC timestamps to local time (and vice versa) during import. It is vital that NetAnalysis is set to the time zone of the suspect system and not that of the forensic examiner's workstation.

In some situations, you may discover browser records from multiple time zones. In this situation, it is difficult to accurately convert between UTC and local time. NetAnalysis has built-in functionality to easily deal with this scenario (see Dealing with Mixed Time Zone Data on Page 90).

To access the time zone settings, select Tools » Options from the Tools menu. Figure 66 shows the Time Zone Settings page.

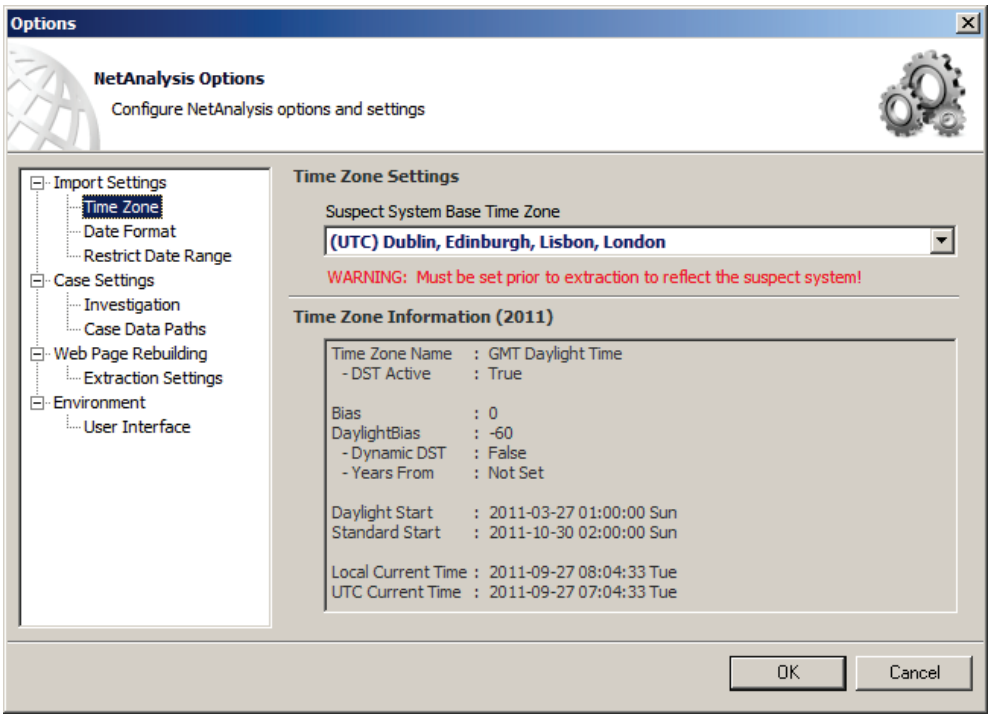


Figure 66

WARNING: If the time zone of the suspect computer is not identified prior to extracting and viewing any Internet history or cache data then the date/time stamps may not be accurately represented!

You MUST establish the correct settings prior to importing any data.

Identification of Suspect Machine Time Zone

When examining a Microsoft Windows NT system, the time zone information can be established by reviewing the SYSTEM registry hive. To enable us to identify the correct Time Zone Information sub-key, we need to establish which Control Set was active when the computer was seized.

ControlSets

A control set contains system configuration information such as device drivers and services [3]. You may notice several instances of control sets when viewing the registry. Some are duplicates or mirror images of others and some are unique.

Control sets are stored in the HKEY_LOCAL_MACHINE sub tree, under the SYSTEM key. There may be several control sets depending on how often the user changed their system. A typical installation of Windows NT will contain three:

Windows NT Control Sets
HKEY_LOCAL_MACHINE\System\ControlSet001
HKEY_LOCAL_MACHINE\System\ControlSet002
HKEY_LOCAL_MACHINE\System\CurrentControlSet

Table 15

ControlSet001 may be the last control set the system booted with, while ControlSet002 could be what is known as the last known good control set, or the control set that last successfully booted Windows NT.

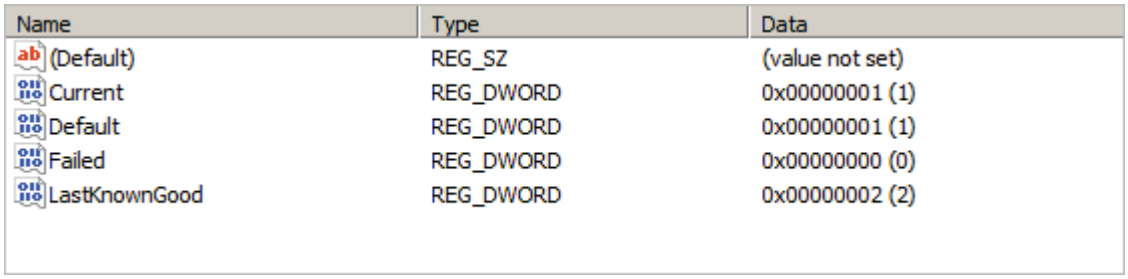
The CurrentControlSet sub-key is a pointer to one of the ControlSetXXX keys and will only be visible when viewing a live registry. During a post-mortem examination, this key will not exist. In order to better understand how these control sets are used, you need to be aware of another sub-key, ‘Select’.

Windows NT Select Key
HKEY_LOCAL_MACHINE\System\Select

Table 16

The Select sub-key contains the values (as can be seen in Figure 67) Current, Default, Failed and LastKnownGood.

Each of these values contains a REG_DWORD data type and refers to a specific control set. For example, if the Current value is set to 0x01, then CurrentControlSet would be pointing to ControlSet001. Similarly, if LastKnownGood was set to 0x02, then the last known good control set would be ControlSet002. The Default value usually agrees with Current, and Failed refers to a control set that was unable to boot Windows NT successfully.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownGood	REG_DWORD	0x00000002 (2)

Figure 67

The most valuable set is CurrentControlSet as that reflects the active control set at the time the system was last active. If we examine the SYSTEM hive from our case, we can see that the CurrentControlSet value is 0x01 which reflects ControlSet001 (see Figure 67).

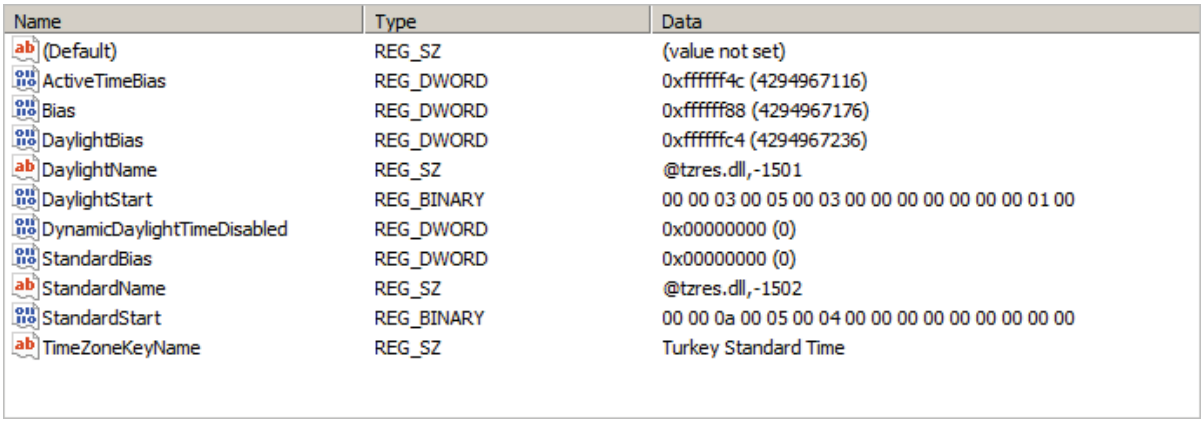
Time Zone Information Sub-Key

Now that the CurrentControlSet has been identified, we can navigate to the sub-key containing the time zone information (see Table 17).

Windows NT TimeZoneInformation Sub-Key
HKEY_LOCAL_MACHINE\ControlSet001\Control\TimeZoneInformation

Table 17

Figure 68 shows the various values stored under this sub-key.



Name	Type	Data
(Default)	REG_SZ	(value not set)
ActiveTimeBias	REG_DWORD	0xffffff4c (4294967116)
Bias	REG_DWORD	0xffffff88 (4294967176)
DaylightBias	REG_DWORD	0xfffffffc4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-1501
DaylightStart	REG_BINARY	00 00 03 00 05 00 03 00 00 00 00 00 00 00 01 00
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-1502
StandardStart	REG_BINARY	00 00 0a 00 05 00 04 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Turkey Standard Time

Figure 68

ActiveTimeBias

This value is the current time difference from UTC in minutes, regardless of whether daylight saving is in effect or not. It is this value that helps establish the current time zone settings.

Bias

This value is the normal time difference from UTC in minutes. This value is the number of minutes that would need to be added to local time to return a UTC value.

StandardBias

This value is added to the value of the Bias member to form the bias used during standard time. In most time zones the value of this member is zero.

DaylightBias

This value specifies a bias value to be used during local time translations that occur during daylight time. This value is added to the value of the Bias member to form the bias used during daylight time. In most time zones the value of this member is -60.

The ActiveTimeBias determines the offset of local time from UTC and is a dynamic value. It is calculated based on the values of the Bias, StandardBias and DaylightBias dependent upon whether Standard Time is in operation or not.

ActiveTimeBias Calculations for DST and Standard Time	
Daylight Saving	ActiveTimeBias = Bias + DaylightBias
Standard Time	ActiveTimeBias = Bias + StandardBias

Table 18

Table 18 shows the calculations for establishing the ActiveTimeBias during Daylight Saving and Standard Time.

Table 19 shows the calculations for converting between UTC and local time using the ActiveTimeBias. It is also possible to calculate the ActiveTimeBias when a UTC and local time are known.

UTC / Local Time Calculations with ActiveTimeBias
UTC = LocalTime + ActiveTimeBias
LocalTime = UTC - ActiveTimeBias
ActiveTimeBias = UTC - LocalTime

Table 19

DaylightName

The operating system uses this name during daylight saving months to display the current time zone setting (see Returning Daylight / Standard Name Values on Page 86).

DaylightStart

This binary data is stored in a SYSTEMTIME structure; it is used to identify the date/time that daylight saving will commence for this time zone.

StandardName

The operating system uses this name during non-daylight saving months to display the current time zone setting (see Returning Daylight / Standard Name Values on Page 86).

StandardStart

This binary data is stored in a SYSTEMTIME structure; it is used to identify the date/time that standard time will commence for this time zone.

DynamicDaylightTimeDisabled

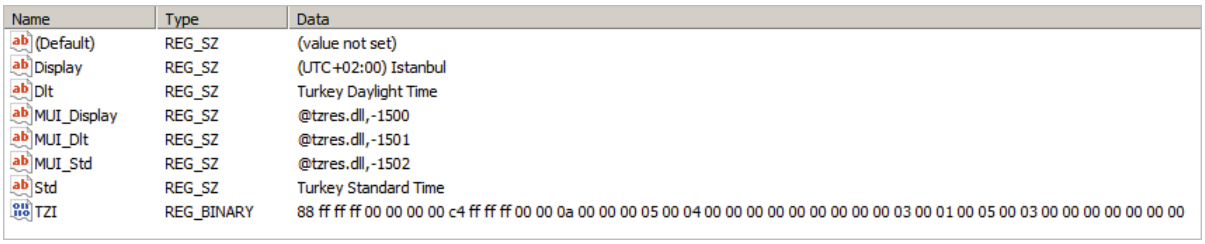
This is a Boolean value which indicates whether a DST adjustment is to be applied.

TimeZoneKeyName

This string relates to the sub-key in the SYSTEM hive where all of the available time zones are stored on a Windows NT system (see Table 20).

Table 20

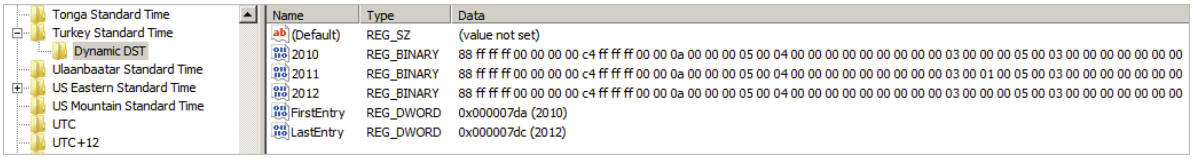
Figure 69 shows the Turkey Standard Time sub-key.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Display	REG_SZ	(UTC+02:00) Istanbul
Dlt	REG_SZ	Turkey Daylight Time
MUI_Display	REG_SZ	@tzres.dll,-1500
MUI_Dlt	REG_SZ	@tzres.dll,-1501
MUI_Std	REG_SZ	@tzres.dll,-1502
Std	REG_SZ	Turkey Standard Time
TZI	REG_BINARY	88 ff ff ff 00 00 00 00 c4 ff ff ff 00 00 0a 00 00 00 05 00 04 00 00 00 00 00 00 00 00 00 03 00 01 00 05 00 03 00 00 00 00 00 00 00

Figure 69

Directly below the Turkey Standard Time sub-key, there is a Dynamic DST sub-key. This holds information and structures relating to the dynamic DST settings.



- Tonga Standard Time
- Turkey Standard Time
  - Dynamic DST
- Ulaanbaatar Standard Time
- US Eastern Standard Time
- US Mountain Standard Time
- UTC
- UTC+12

Name	Type	Data
(Default)	REG_SZ	(value not set)
2010	REG_BINARY	88 ff ff ff 00 00 00 00 c4 ff ff ff 00 00 0a 00 00 00 05 00 04 00 00 00 00 00 00 00 00 00 03 00 00 00 05 00 03 00 00 00 00 00 00 00
2011	REG_BINARY	88 ff ff ff 00 00 00 00 c4 ff ff ff 00 00 0a 00 00 00 05 00 04 00 00 00 00 00 00 00 00 00 03 00 01 00 05 00 03 00 00 00 00 00 00 00
2012	REG_BINARY	88 ff ff ff 00 00 00 00 c4 ff ff ff 00 00 0a 00 00 00 05 00 04 00 00 00 00 00 00 00 00 00 03 00 00 00 05 00 03 00 00 00 00 00 00 00
FirstEntry	REG_DWORD	0x000007da (2010)
LastEntry	REG_DWORD	0x000007dc (2012)

Figure 70

Dynamic DST

The implementation of Daylight Saving Time varies from country to country. Some countries may not observe Daylight Saving Time, whereas other countries may change the start dates and end dates for Daylight Saving Time every year.

Dynamic Daylight Saving Time provides support for time zones whose boundaries for Daylight Saving Time change from year to year. This feature enables easier updating of systems, especially for locales where the yearly DST boundaries are known in advance.

After the time zone has been updated, the current time zone setting is applied to all time operations, even when the time in question occurred before the time zone changed.

SYSTEMTIME Structure

The value containing the start date/time for DaylightStart or StandardStart is stored in a common structure called SYSTEMTIME. This structure specifies a date and time, using individual members for the month, day, year, weekday, hour, minute, second, and millisecond. Figure 71 shows the structure.

```
typedef struct _SYSTEMTIME {
  WORD wYear;
  WORD wMonth;
  WORD wDayOfWeek;
  WORD wDay;
  WORD wHour;
  WORD wMinute;
  WORD wSecond;
  WORD wMilliseconds;
} SYSTEMTIME, *PSYSTEMTIME
```

Figure 71

In our example (see Figure 72), the DaylightStart value is a REG_BINARY value containing a number of bytes. These bytes represent the various elements of the SYSTEMTIME structure. The WORD values are stored in Little Endian format.

Figure 72

Figure 72 shows the binary value for DaylightStart. Each WORD from the SYSTEMTIME structure is broken down in Table 21.

Bytes	Value	Information
Bytes 0 - 1	0x0000	Represent the year from a 1900 time base. This is only required if the change is year specific and will normally be zero.
Bytes 2 - 3	0x0003	Represent the month; in this case the third month is March.
Bytes 4 - 5	0x0005	Represent the week (starts at 1 and 5 means last); in this case the last week.
Bytes 6 - 7	0x0003	Represents the hour; in this case 0300 hours.
Bytes 8 - 9	0x0000	Represents the minute value; in this case zero.

Bytes	Value	Information
Bytes 10 - 11	0x0000	Represent the second value; in this case zero.
Bytes 12 - 13	0x0000	Represents the millisecond value; in this case zero.
Bytes 14 - 15	0x0001	Represents the day of the week (Sunday = 0); in this case Monday.

Table 21

In our scenario, Daylight Saving Time (DST) will start on Monday of the last week in March at 0300 hours. Using the same calculation, we can calculate that Standard Time will start on Sunday of the last week in October at 0400 hours.

Calculating Signed Integer Bias Values

Within digital systems, all data, whether they are numbers or characters are represented by binary digits. A problem arises when you want to store negative numbers.

Over the years, hardware designers have developed three different schemes for representing negative numbers: sign and magnitude, one's complement, and two's complement. The most common method for storing negative numbers is two's complement. With this method, the Most Significant Bit (MSB) is used to store the sign. If the MSB is set, then this represents a negative number. This method affords natural arithmetic operations with no special rules. To represent a negative number in twos complement notation the process is simple:

- Find the binary representation of the positive (+ve) value in n-bits
- Flip all the bits (change 1 to 0 and vice versa)
- Add 1

Figure 73 below shows the binary representation of the positive number 5.

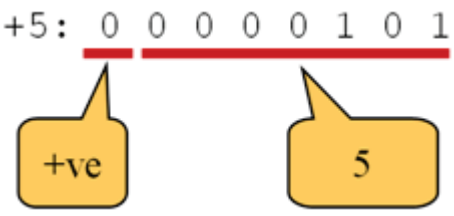


Figure 73

To represent this as a negative number (using 8 bits) then the procedure above is followed. Flip the bits as shown above and add one as shown in Figure 74.

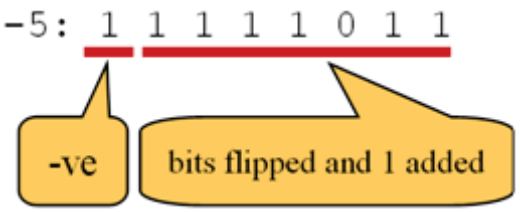


Figure 74

This method makes it simple to add positive and negative numbers together; for example:

```
-5:    11111011
+5:   +00000101
      ---------
       00000000
```

Figure 75

It also makes it very easy to convert between positive and negative numbers:

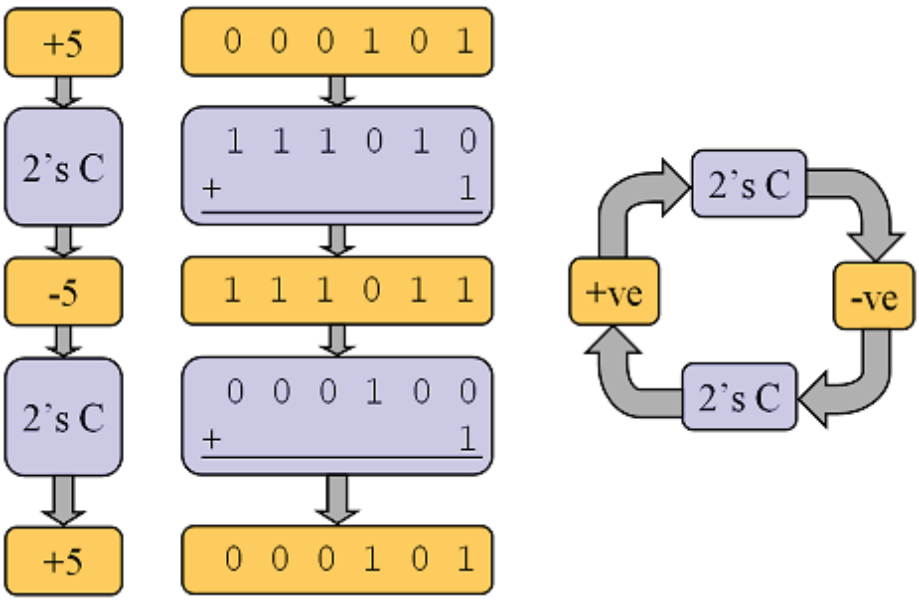


Figure 76

ActiveTimeBias

The ActiveTimeBias information is stored in the Time Zone Information sub-key as a REG_DWORD signed integer value. This value may be positive or negative. To establish the true value of the key, we must examine the information stored (see Figure 77).

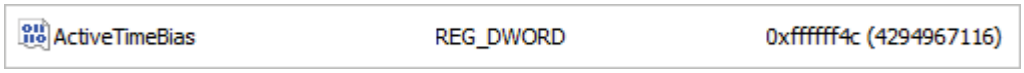


Figure 77

As the REG_DWORD value can store both signed and unsigned values, with no way to differentiate between each type, it is displayed in the Registry viewer as an unsigned value. To establish the two's complement value, we must carry out the following calculation:

```
0xFFFFFF4C (Signed Integer Value)
```

Figure 78

Convert this to binary:

```
11111111 11111111 11111111 01001100
```

Figure 79

The MSB is set so we know that the above value will be negative. The next stage is to flip all the bits. This involves changing 1 to 0 and vice versa. This can be achieved quickly using the logical NOT function on a scientific calculator. You must ensure that it is set to deal with the correct number of bits.

```
00000000 00000000 00000000 10110011
```

Figure 80

Add 1 bit to the value above:

```
10110100
```

Figure 81

And then convert that value back to decimal, remembering that we are dealing with a negative number:

```
-180 (Minus 180)
```

Figure 82

If the MSB had been zero, then the value would have been positive. With a positive value, just convert it directly to decimal. If using a scientific calculator and using the logical NOT operator, ensure you are dealing with DWORD (32 bits).

Bias Calculations

Examination of the Bias values in our example indicates that DST is active and the local time for that zone is 3 hours ahead of UTC (see Table 22).

Bias	HEX Value	DEC Value	Information
ActiveTimeBias	0xFFFFFF4C	-180	Current local time is 3 hours ahead of UTC (shows DST active)
Bias	0xFFFFFF88	-120	2 hours ahead of UTC during Standard Time
DaylightBias	0xFFFFFFC4	-60	1 hour ahead of Standard Time when DST active
StandardBias	0x00000000	0	No change for Standard Time

Table 22

Returning Daylight / Standard Name Values

In earlier versions of Windows NT, both DaylightName and StandardName values contain the actual strings relating to those items. In later versions, these values were changed to reference a string of text stored within a string table embedded within a DLL (see Figure 83).

Name	Type	Data
DaylightName	REG_SZ	@tzres.dll,-1501
StandardName	REG_SZ	@tzres.dll,-1502

Figure 83

For Windows 7, the string table is contained within a dynamic link library called 'tzres.dll'. If this file is opened in a resource viewer, we can examine the string table values. Figure 84 shows a small part of the string table when viewed from Microsoft Visual Studio. In Figure 83, DaylightName is stored as string 1501, with StandardName stored as string 1502. The corresponding values in the string table show 'Turkey Daylight Time' and 'Turkey Standard Time' (see Figure 69 on Page 81 for further references to this string table).

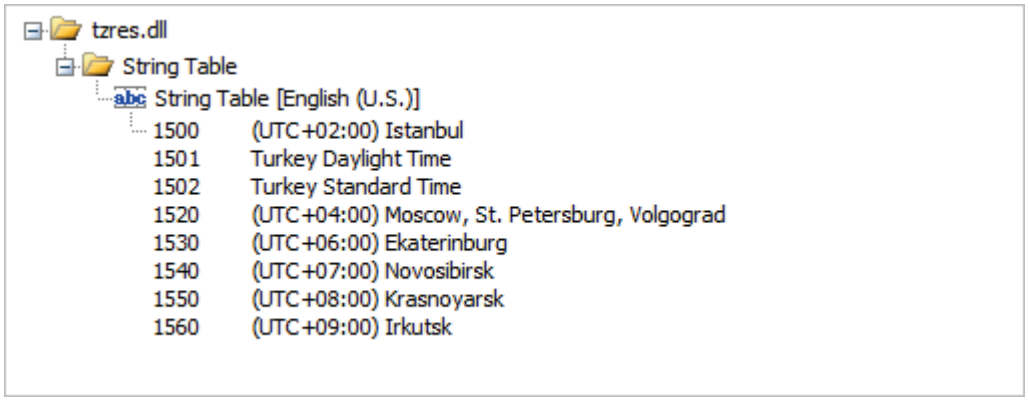


Figure 84

NetAnalysis ActiveBias Column

Another method to verify that the time zone settings are correct is to open a Microsoft Internet Explorer Daily INDEX.DAT file. In this INDEX.DAT file, there are two dates stored; one in local time and one in UTC (see Figure 85). NetAnalysis does not apply any time zone change to this file type as it already contains a UTC and local time value.

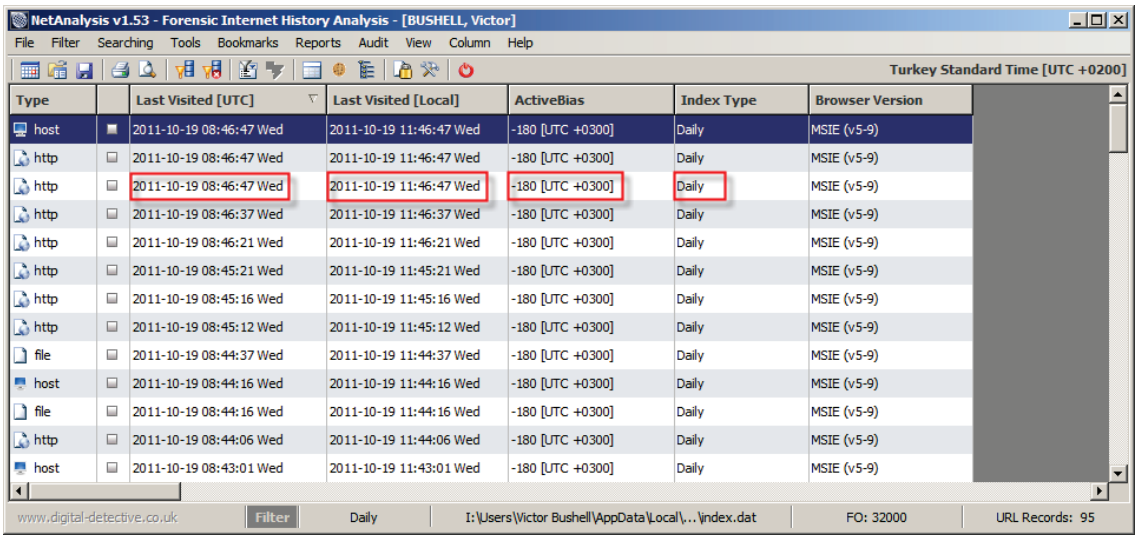


Figure 85

Table 23 shows the Last Visit [UTC] and Last Visit [Local] timestamps from the outlined record in Figure 85. The difference between UTC and local time is 180 minutes. As the local time is 180 minutes ahead of UTC, the ActiveBias is minus 180 (-180 minutes). This corresponds with the information recovered from the registry in Table 22.

UTC Time	Local Time	Local Time Difference	ActiveBias
08:46:47 Hours	11:46:47 Hours	3 Hours (180 minutes) ahead of UTC	-180 Minutes

Table 23

Time Zone Warnings

As NetAnalysis imports data from Microsoft Internet Explorer Daily INDEX.DAT records, it checks the bias difference between the last visited UTC and local times and adds the calculated bias to the ActiveBias column. This information is checked against the bias information for the time zone set (in NetAnalysis Options) by the examiner. If the time zone has not been set correctly, or there are multiple time zone bias values encountered, NetAnalysis will flag this when it completes importing the INDEX data.

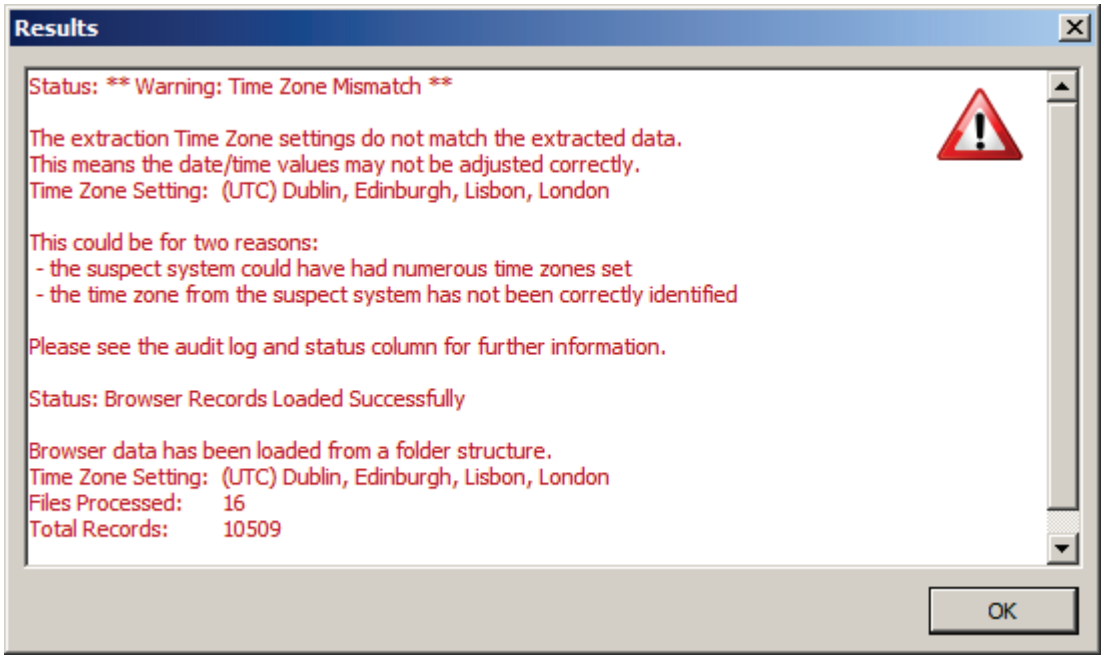


Figure 86

To establish where the problem lies, examine the ActiveBias column as shown in Figure 87. The ActiveBias column shows the bias for the highlighted record is -180 minutes [UTC +0300].

We can also see that for this import, the time zone was set to GMT Standard Time [UTC +0000]. The asterisk [*] symbol after the ActiveBias value indicates there is a problem and to review the Status column. The Status column shows there is an issue with the time zone settings.

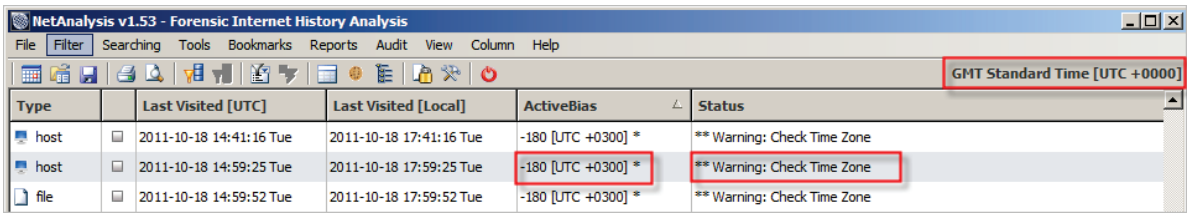


Figure 87

At this point, it is advisable to review the content of the audit Log. This can be accessed from the Audit Log button on the main toolbar, or from the menu: Audit » View Audit Log. Figure 88 shows a portion of the audit log with a time zone warning highlighted.

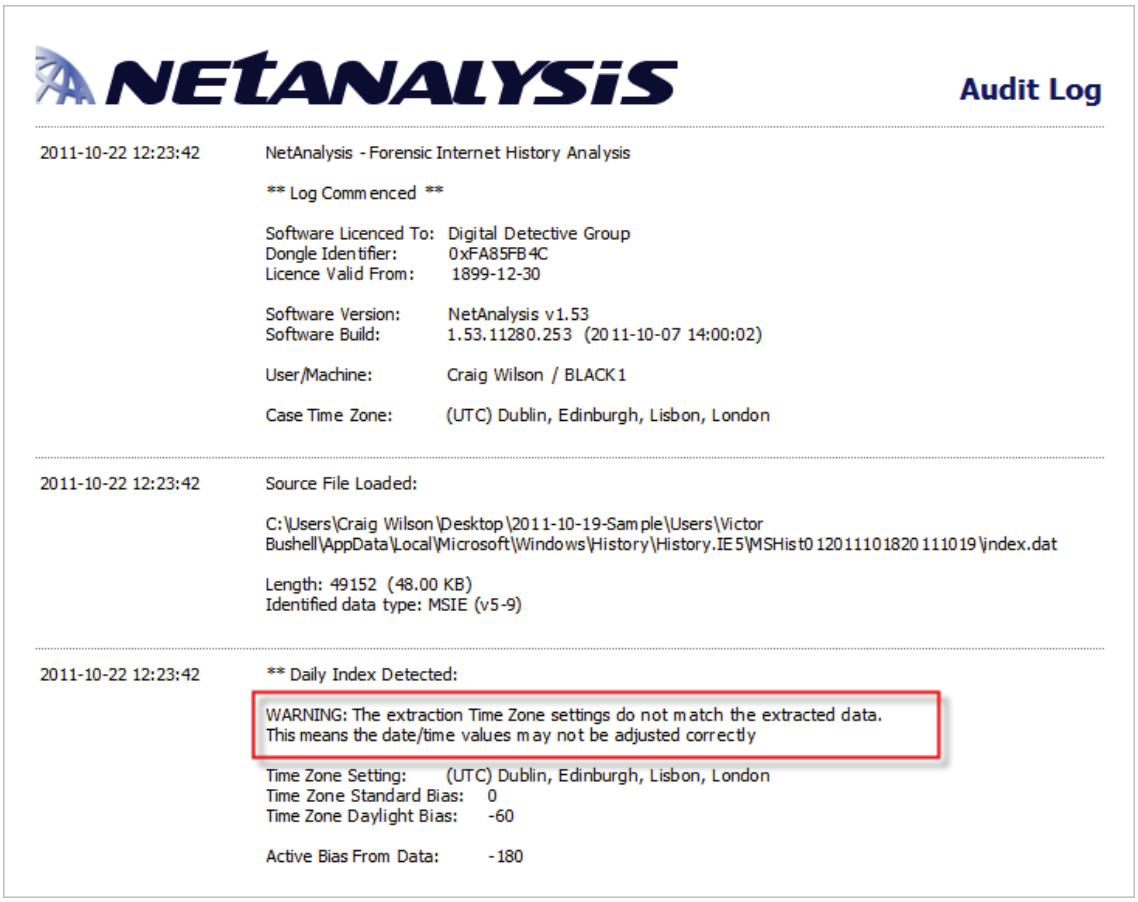


Figure 88

It is clear from the information presented by NetAnalysis that the importation time zone setting is incorrect. Examination of the ActiveBias column also shows that there appears to be only one bias value identified. This indicates a single time zone setting but an incorrect import setting for NetAnalysis. In this case, you would simply check the time zone settings, select the correct value and then re-import the data.

Dealing with Mixed Time Zone Data

If you have evidence of multiple time zones being set, you will end up with miscalculated timestamps if you select any of the standard time zone settings.

The recommended course of action in this case is to set the NetAnalysis time zone option to 'No Time Zone Date / Time Adjustment'. With this setting, NetAnalysis will calculate the date/times exactly as they are stored in the file. You can then re-import the data into NetAnalysis. NetAnalysis will only represent what it knows to be accurate (assuming the clock was accurate on the system and the computer was being used in the time zone it was set to use).

To access the time zone settings, select Tools » Options from the Tools menu. Select '* No Time Zone Date/Time Adjustment' from the Suspect System Base Time Zone dropdown list (as shown in Figure 89).

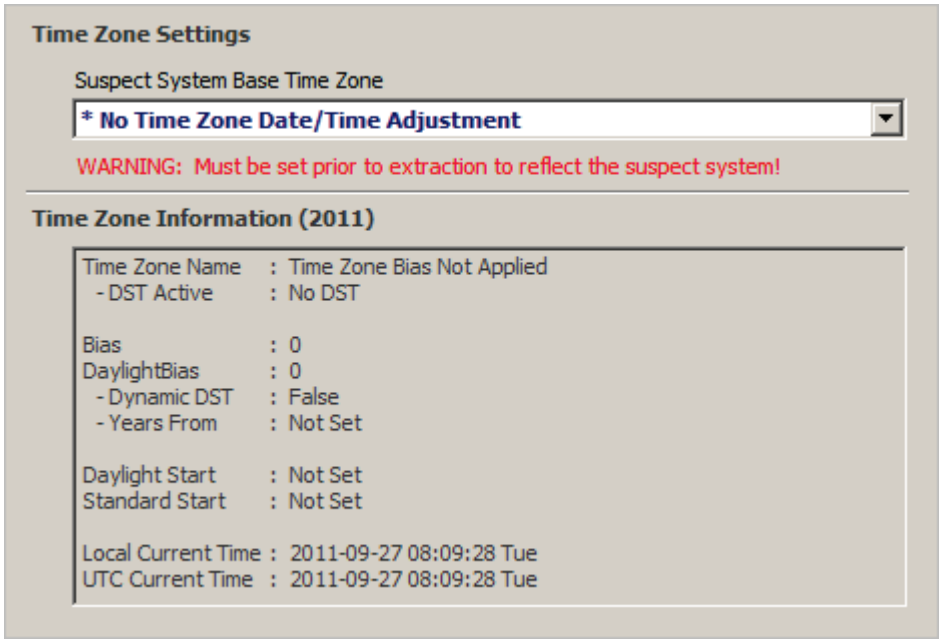


Figure 89

Location of Browser Data

Internet Explorer: Windows XP

Cookies

```
C:\Documents and Settings\{user}\Cookies\index.dat
```

History

```
C:\Documents and Settings\{user}\Local Settings\History\History.IE5\index.dat
C:\Documents and Settings\{user}\Local Settings\History\History.IE5\MSHist01YYYYMMDDYYYYMMDD\index.dat
```

Cache

```
C:\Documents and Settings\{user}\Local Settings\Temporary Internet Files\Content.IE5\index.dat
```

Other

```
C:\Documents and Settings\{user}\IETldCache\index.dat
C:\Documents and Settings\{user}\PrivacIE\index.dat
C:\Documents and Settings\{user}\Local Settings\Application Data\Microsoft\Feeds Cache\index.dat
C:\Documents and Settings\{user}\Local Settings\Application Data\Microsoft\Internet Explorer\DOMStore\index.dat
```

Internet Explorer: Windows Vista/7

AppData\Local\Microsoft

```
C:\Users\{user}\AppData\Local\Microsoft\Feeds Cache\index.dat
C:\Users\{user}\AppData\Local\Microsoft\Internet Explorer\DOMStore\index.dat
```

AppData\Local\Microsoft\Windows\History

```
C:\Users\{user}\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Users\{user}\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist01YYYYMMDDYYYYMMDD\index.dat
C:\Users\{user}\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat
```

AppData\Local\Microsoft\Windows\Temporary Internet Files

```
C:\Users\{user}\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\{user}\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\index.dat
```

AppData\Local\Temp\Low

```
C:\Users\{user}\AppData\Local\Temp\Low\Cookies\index.dat
C:\Users\{user}\AppData\Local\Temp\Low\History\History.IE5\index.dat
C:\Users\{user}\AppData\Local\Temp\Low\Temporary Internet Files\Content.IE5\index.dat
```

AppData\LocalLow

```
C:\Users\{user}\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\index.dat
```

AppData\Roaming

```
C:\Users\{user}\AppData\Roaming\Microsoft\Internet Explorer\UserData\index.dat
C:\Users\{user}\AppData\Roaming\Microsoft\Internet Explorer\UserData\Low\index.dat
C:\Users\{user}\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\{user}\AppData\Roaming\Microsoft\Windows\Cookies\Low\index.dat
C:\Users\{user}\AppData\Roaming\Microsoft\Windows\IECompatCache\index.dat
C:\Users\{user}\AppData\Roaming\Microsoft\Windows\IECompatCache\Low\index.dat
C:\Users\{user}\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\index.dat
C:\Users\{user}\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat
C:\Users\{user}\AppData\Roaming\Microsoft\Windows\IETldCache\Low\index.dat
C:\Users\{user}\AppData\Roaming\Microsoft\Windows\PrivacIE\index.dat
C:\Users\{user}\AppData\Roaming\Microsoft\Windows\PrivacIE\Low\index.dat
```

Apple Safari: Windows XP

History

```
C:\Documents and Settings\{user}\Application Data\Apple Computer\Safari\
```

Cache

```
C:\Documents and Settings\{user}\Local Settings\Application Data\Apple Computer\Safari\
```

Apple Safari: Windows Vista/7

History

```
C:\Users\{user}\AppData\Roaming\Apple Computer\Safari\
```

Cache

```
C:\Users\{user}\AppData\Local\Apple Computer\Safari\
```

Apple Safari: Apple Macintosh OS X 10.6

History

```
/Users/{user}/Library/Safari/
```

Cache

```
/Users/{user}/Library/Caches/com.apple.Safari/
```

Mozilla Firefox: Windows XP

History and Downloads

```
C:\Documents and Settings\{user}\Application Data\Mozilla\Firefox\Profiles\{profile folder}\
```

Cache

```
C:\Documents and Settings\{user}\Local Settings\Application Data\Mozilla\Firefox\Profiles\{profile folder}\Cache\
```

Mozilla Firefox: Windows Vista/7

History and Downloads

```
C:\Users\{user}\AppData\Roaming\Mozilla\Firefox\Profiles\{profile folder}\
```

Cache

```
C:\Users\{user}\AppData\Local\Mozilla\Firefox\Profiles\{profile folder}\Cache\
```

Mozilla Firefox: Apple Macintosh OS X 10.6

History and Downloads

```
/Users/{user}/Library/Application Support/Firefox/Profiles/{profile folder}/
```

Cache

```
/Users/{user}/Library/Caches/Firefox/Profiles/{profile folder}/Cache/
```

Mozilla Firefox: GNU/Linux

History and Downloads

```
/home/{user}/.mozilla/firefox/{profile folder}/
```

Cache

```
/home/{user}/.mozilla/firefox/{profile folder}/Cache/
```

Google Chrome: Windows XP

History

```
C:\Documents and Settings\{user}\Local Settings\Application Data\Google\Chrome\User Data\Default\
```

Cache

```
C:\Documents and Settings\{user}\Local Settings\Application Data\Google\Chrome\User Data\Default\Cache\
```

Google Chrome: Windows Vista/7

History

```
C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default\
```

Cache

```
C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default\Cache\
```

Google Chrome: Apple Macintosh OS X 10.6

History

```
/Users/{user}/Library/Application Support/Google/Chrome/Default/
```

Cache

```
/Users/{user}/Library/Caches/Google/Chrome/Default/Cache/
```

Google Chrome: GNU/Linux

History

```
/home/{user}/.config/google-chrome/Default/
```

Cache

```
/home/{user}/.cache/google-chrome/Default/Cache/
```

Opera: Windows XP

History

```
C:\Documents and Settings\{user}\Application Data\Opera\Opera\
```

Cache

```
C:\Documents and Settings\{user}\Local Settings\Application Data\Opera\Opera\cache\
```

Opera: Windows Vista/7

History

```
C:\Users\{user}\AppData\Roaming\Opera\Opera\
```

Cache

```
C:\Users\{user}\AppData\Local\Opera\Opera\cache\
```

Opera: Apple Macintosh OS X 10.6

History

```
/Users/{user}/Library/Opera/
```

Cache

```
/Users/{user}/Library/Caches/Opera/cache/
```

Opera: GNU/Linux

History

```
/home/{user}/.opera/
```

Cache

```
/home/{user}/.opera/cache/
```

NetAnalysis Quick Start

Before You Start

Prior to importing any data, or in fact, dealing with live evidence, please ensure you have read the following chapters (as shown in Table 24).

Chapter Title	Page Number
Introduction to NetAnalysis™	9
Installing NetAnalysis	29
Installing a Licence Key File	44
USB Hardware Dongles	45
Practice Files	49
NetAnalysis: A Guided Tour	50
Configuring NetAnalysis	70
Time Zone Configuration	75

Table 24

We have provided a set of practice files to allow you to work through the various features of NetAnalysis; it is recommended you become familiar with the software through examining the practice files before accessing live evidence.

To download the practice files, please follow the instructions on Page 49.

Establishing the Suspect Time Zone

In the forensic examination of a digital device, establishing the time zone is one of the first things a forensic examiner should do. If this information is not established at an early stage and taken into account, then the validity of all date/time values may be brought into question.

It is also vital that the digital forensic examiner understands the difference between Local and Coordinated Universal Time (UTC). This is explained fully in the chapter: Time Zone Configuration on Page 75.

WARNING: If the time zone of the suspect computer is not identified prior to extracting and viewing any Internet history or cache data then the date/time stamps may not be accurately represented!

You MUST establish the correct settings prior to importing any data.

In the file structure of the practice files, there is a SYSTEM registry hive. Using the information from the Time Zone Configuration Chapter on Page 75, examine the hive and establish which time zone this laptop was set to when it was seized.

Setting the Time Zone

If you have examined the registry hive correctly, you will have established that the time zone was set to 'Istanbul (UTC +0200)'.

To set the time zone in NetAnalysis, select Tools » Options from the menu. The Options window should automatically appear with the time zone settings pane in view. Change the 'Suspect System Base Time Zone' to 'Istanbul (UTC +0200)' (as shown in Figure 90).

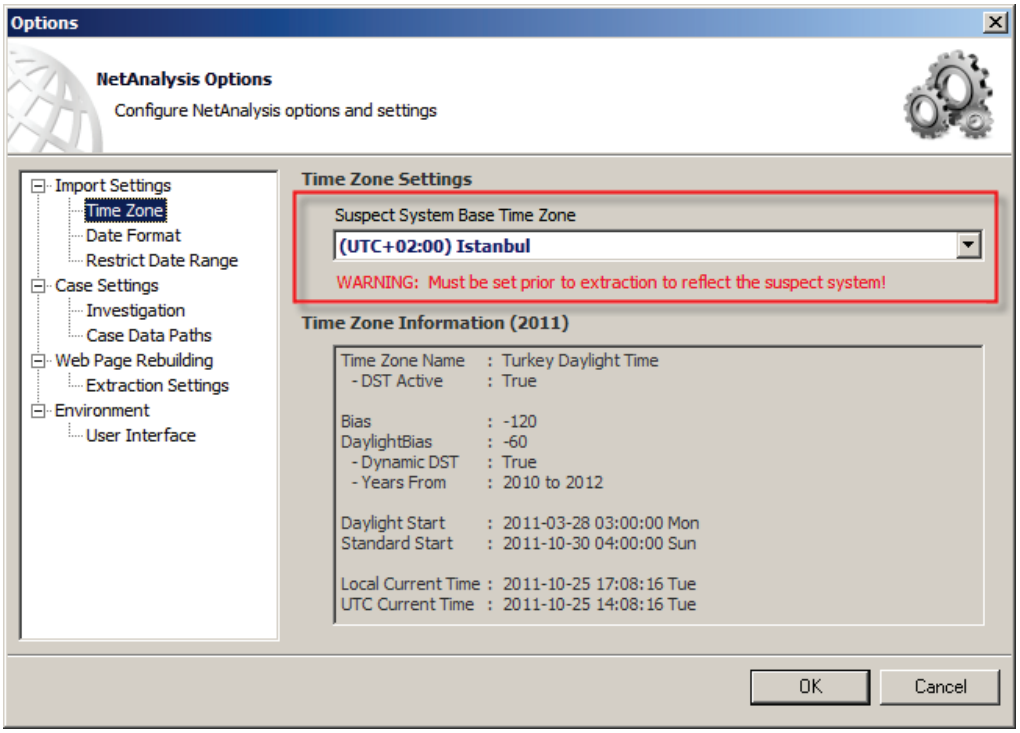


Figure 90

Now click OK to set the time zone for this case.

Importing History Files

There are two main ways to import data into NetAnalysis. The first allows you to open any supported file(s). This can be performed by selecting File » Open History.

When the Open Internet History File window opens, you can change the file filter to only show files for the type of browser you wish to import (see Figure 91).

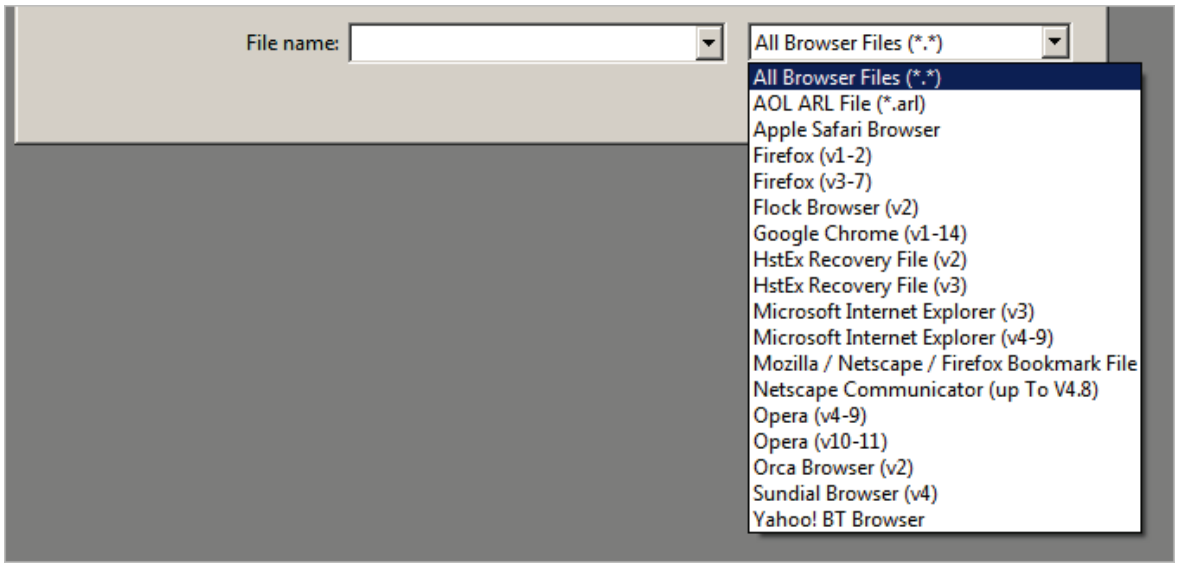


Figure 91

This method is used for opening a specific file or group of files.

Importing History from a Folder Structure

The second (more common) method is to use the 'Open All History from Folder' method. This option will recursively search the file system for supported files and then import any that have been found.

WARNING: Some third party image mounting tools do not deal with NTFS symbolic links correctly within a forensic environment. Testing has identified an issue where NTFS symbolic links on mounted volumes point to folders on the forensic examiners own hard disk.

If you use software (such as NetAnalysis or Anti-Virus software) to recursively search a folder structure from a mounted volume containing symbolic links, the operating system on the forensic workstation may point the software to folders which are not contained within the suspect volume. This is NOT an issue with NetAnalysis, but the mounting software not being suitable for forensic use. See knowledge base article KB80018.

To access the recursive import, select File » Open All History from Folder (as shown in Figure 92).

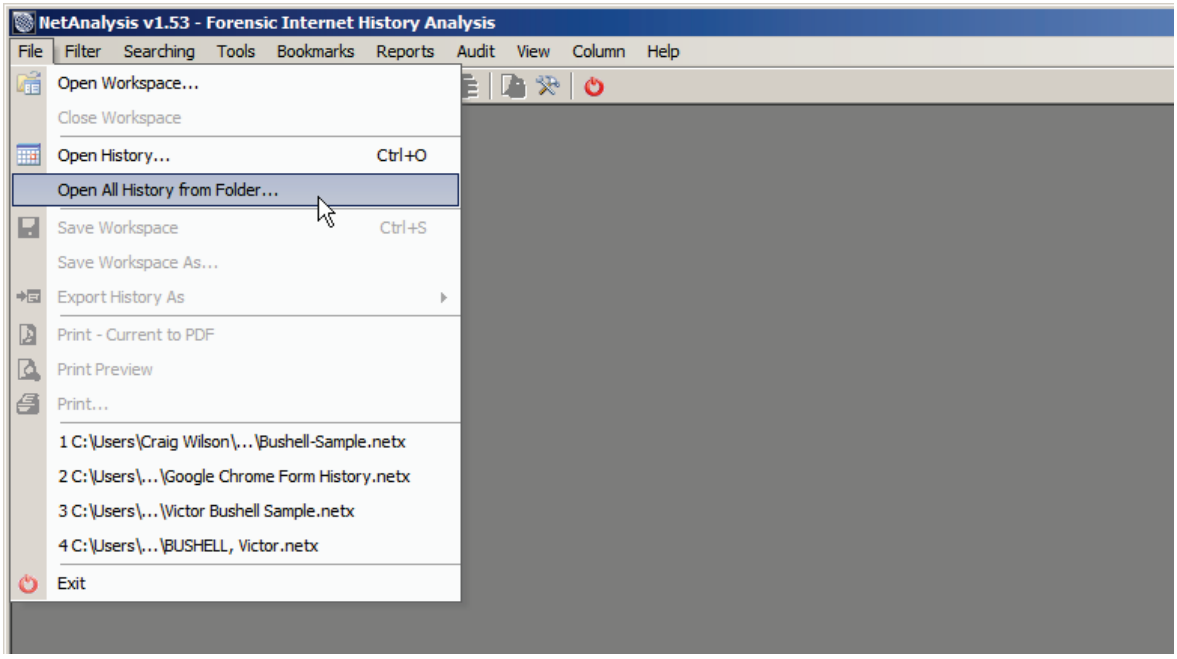


Figure 92

The Browse for Folder window will then open. Navigate to the drive containing your Victor Bushell data, and select the folder containing the user profile (see Figure 93).

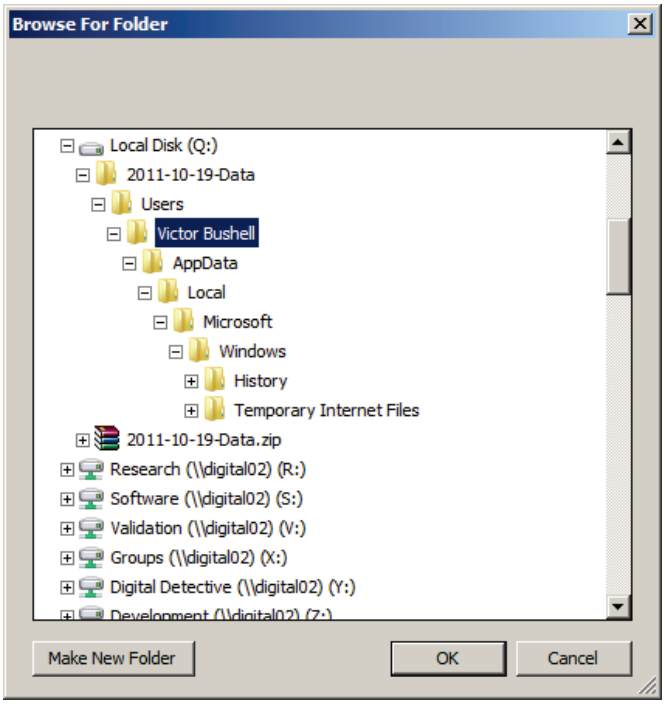


Figure 93

Click OK to start searching through the profile for supported browser files. NetAnalysis should identify 16 possible browser files from this data.

Once each file has been identified, NetAnalysis will start to import each record into the temporary workspace. The progress will be displayed as shown in Figure 94.

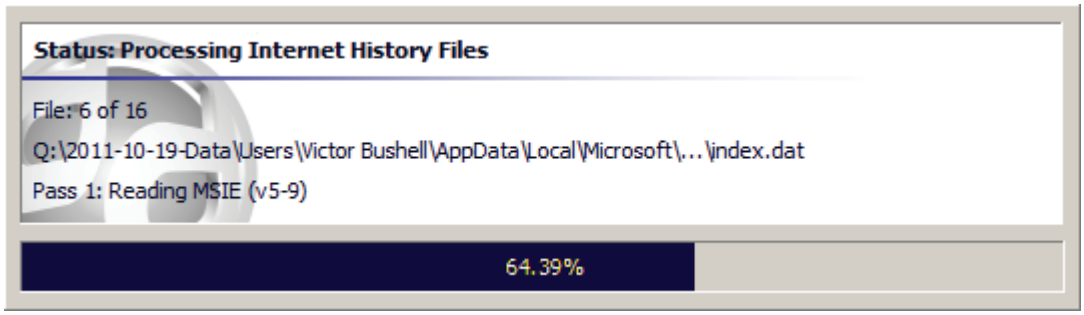


Figure 94

Once the records have been imported, NetAnalysis will display the summary screen as shown in Figure 95. This window shows that all the records have been imported successfully. It shows that 16 files have been imported with a total of 10,509 records identified.

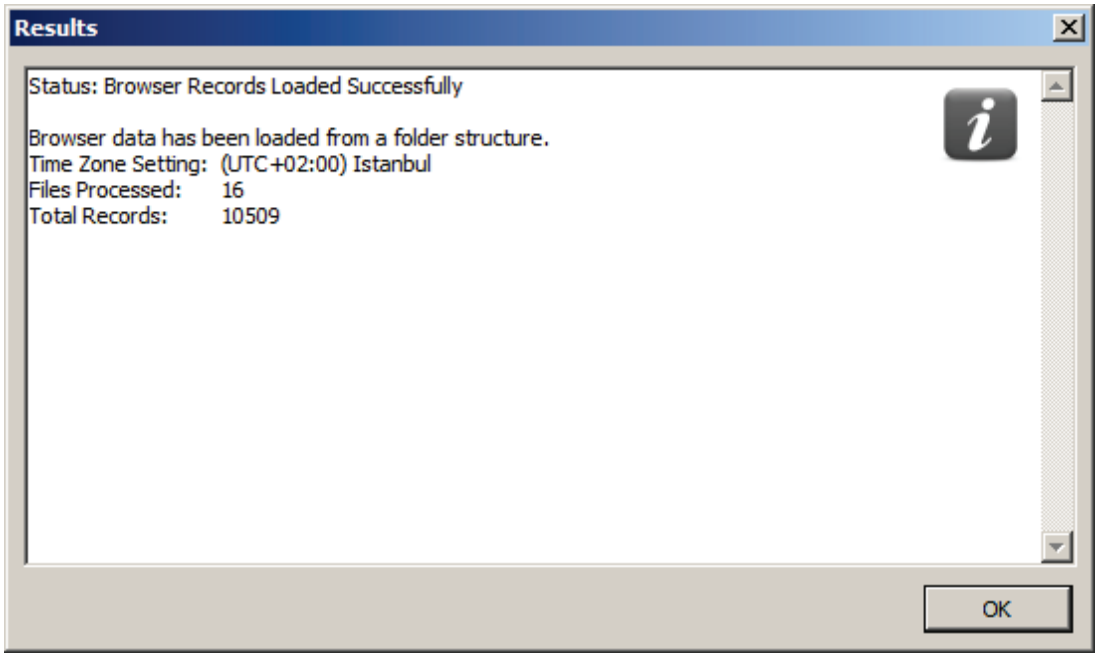


Figure 95

The window also shows that the time zone settings for this import was '(UTC +0200) Istanbul', which is the time zone we set prior to importing any data. This information is also written to the audit log.

You should now have a NetAnalysis window similar to Figure 96 with a total of 10,509 records imported into the workspace.

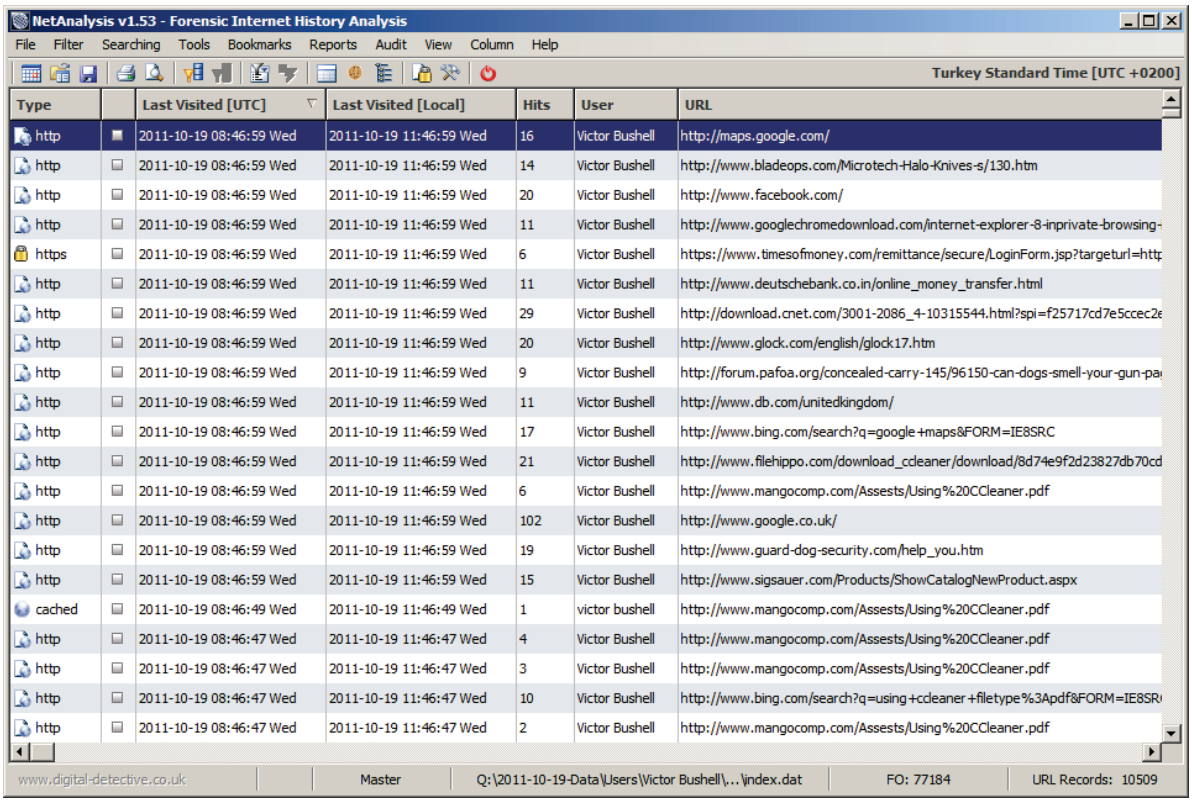


Figure 96

Saving the Workspace

At this point, before you go any further, it is recommended that you save your workspace. Once the workspace has been saved, any modifications such as tagging or bookmarking will be automatically written to the workspace.

To save the workspace, select File » Save Workspace As (or Save Workspace) from the menu. You can also save the workspace by selecting Save from the toolbar.

It may be a good idea at this point to update the case information for this investigation. The case information window can be found by selecting: Tools » Options » Case Settings » Investigation from the menu (see Case Settings: Investigation on Page 72).

You are now ready to start searching and processing the evidence in this case (see Finding the Evidence on Page 103).

Finding the Evidence

Introduction

It is important to be able to quickly identify the Internet history records that are relevant to your investigation. NetAnalysis has a number of different ways to do this:

- Quick Filters
- Multi-Level SQL Filtering
- Keyword Searching
- Column Filter Bar
- Find First, Find Next

In addition to filtering and searching, NetAnalysis also provides a number of different ways to step through, review and bookmark the evidence.

After a filter has been applied, it can be quickly removed by hitting F5, clicking on the Remove Filter button on the toolbar, or selecting the following menu: Filter » Remove Filter - Show All.

The status bar will always show whether a filter is active.

Quick Filter

The quickest way to find specific records within NetAnalysis is to set a quick filter. This will be the normal method for searching, filtering and reviewing.

Filters make it easy to specify which records you want to include in a report or view in the grid. You can select which field (also referred to as a column) to filter along with optional time parameters. You can also set whether you want the search string to match the start of the field, end of the field, whole field or any part of the field. The default setting is for any part of the field. The Filter Text box also remembers the previous 15 strings used to activate filters.

The Filter Form can be activated by clicking on the Show Filter Form button on the toolbar or from the following menu: Searching » Select Filter Criteria. The keyboard shortcut F8 can also be used. This will show the Filter Form, as shown in Figure 97.

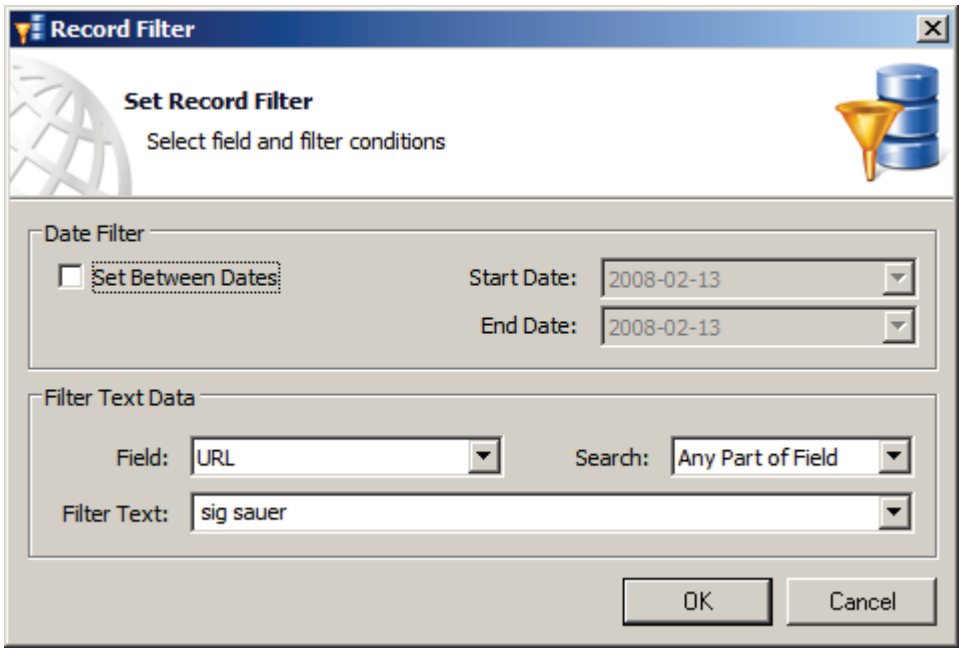


Figure 97

By selecting the 'Set Between Dates' check box, the start and end date fields become active. This allows you to filter the activity between two dates. This date filter will remain active until it is deselected. When you access the Filter form with the date filter activated, you will see the red text "Status: Date Filter Is Active" to warn you that the filter is active (as shown in Figure 98).

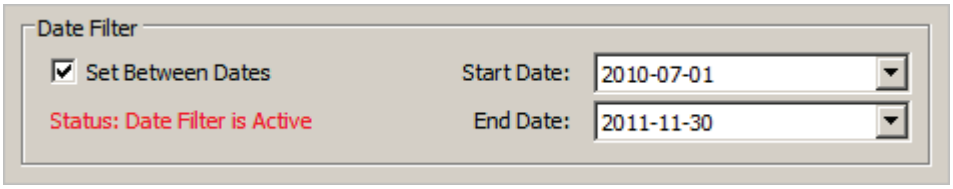


Figure 98

The default field value is URL. This can be changed to any of the other fields by clicking on the drop-down box. The filter type can be changed by clicking on the Search drop-down box. The actual text to be searched for can be entered into the Filter Text box. Clicking 'OK' will activate the desired filter.

The status bar will indicate that a filter is active (see Figure 99). If any of the column headers are then clicked, the order of the records will change whilst maintaining the current filter.

Figure 99

Viewing/Highlighting Keyword Hits

When searching and filtering for data, it is often difficult to see the actual text within the URL. To assist with this, open the URL Examination Window by selecting View » URL Examination Window from the menu. This window will show the whole URL and will highlight the keywords for easy recognition (as shown in Figure 100).

In this example, we searched for the string 'sig sauer'. NetAnalysis automatically generates a search which would filter both words separated by either space separator (%20) or (+).

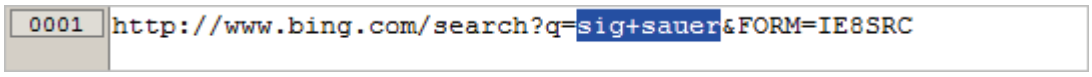


Figure 100

Removing a Filter (F5)

When a filter is active (any filter), it can be removed by pressing the shortcut key F5, clicking the Remove Filter button on the toolbar, or selecting File » Remove Filter - Show All from the Filter menu. NetAnalysis also remembers which record was selected when filters are removed.

Find First URL (F7)

Another quick option for finding URL records is to press the shortcut key F7 and open the Find First form. This can also be activated by selecting Searching » Find First URL Record from the menu.

This form allows you to enter a URL (or part of a URL) and then jump to the first instance containing the string within the workspace. Selecting F3 and F2 allows you to jump back and forward. These options can also be accessed by selecting Searching » Find Next or Searching » Find Previous from the menu.

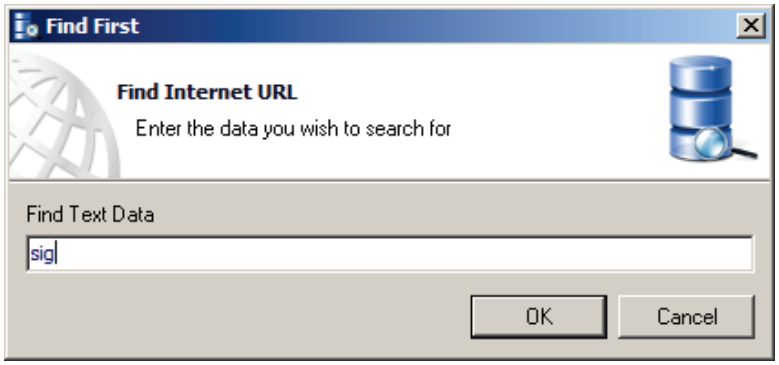


Figure 101

Keyword Lists (F4)

NetAnalysis also has a useful function for searching multiple keywords against the URL, Page Title, Absolute Path or Cache File column. Pressing the F4 shortcut key activates the Keyword List window (as shown in Figure 102). It can also be activated by selecting Searching » User Keyword List from the menu.

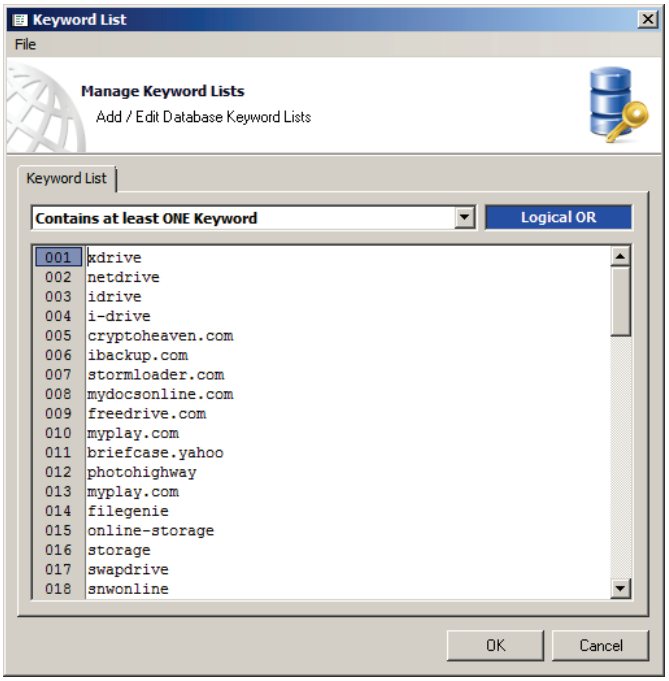


Figure 102

Keyword lists can be saved for later use or shared with other NetAnalysis users. There are also a number of example keyword lists provided with the full installation. These example keyword lists can be opened by selecting File » Open Keyword List (as shown in Figure 103).

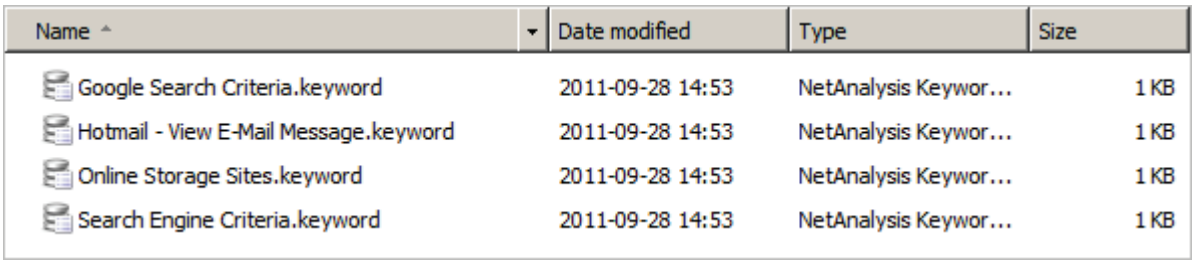


Figure 103

When you have built a keyword list, it can be saved and re-used at a later date. To save a keyword list, select File » Save Keyword List As from the menu.

Searching with Logical Operators

When adding keywords to the list, you have an additional option to select a logical AND/OR operator. With AND searching, every keyword must be present in the field you are searching. With the OR search, at least one of the keywords needs to be present. This allows you to easily search for a list of domains or to build up the required components for a specific URL (such as a web search).

Once you have built (and saved if required) a keyword list, it can be searched against the current workspace by selecting the following menu options:

- Searching » Execute Keyword Search - URL
- Searching » Execute Keyword Search - Page Title
- Searching » Execute Keyword Search - Cache File
- Searching » Execute Keyword Search - Absolute Path

SQL Query Builder (CTRL + F4)

One of the most powerful functions for filtering can be activated by using the SQL Query builder. With the query builder, the user can create powerful SQL filter queries to return only the records they need.

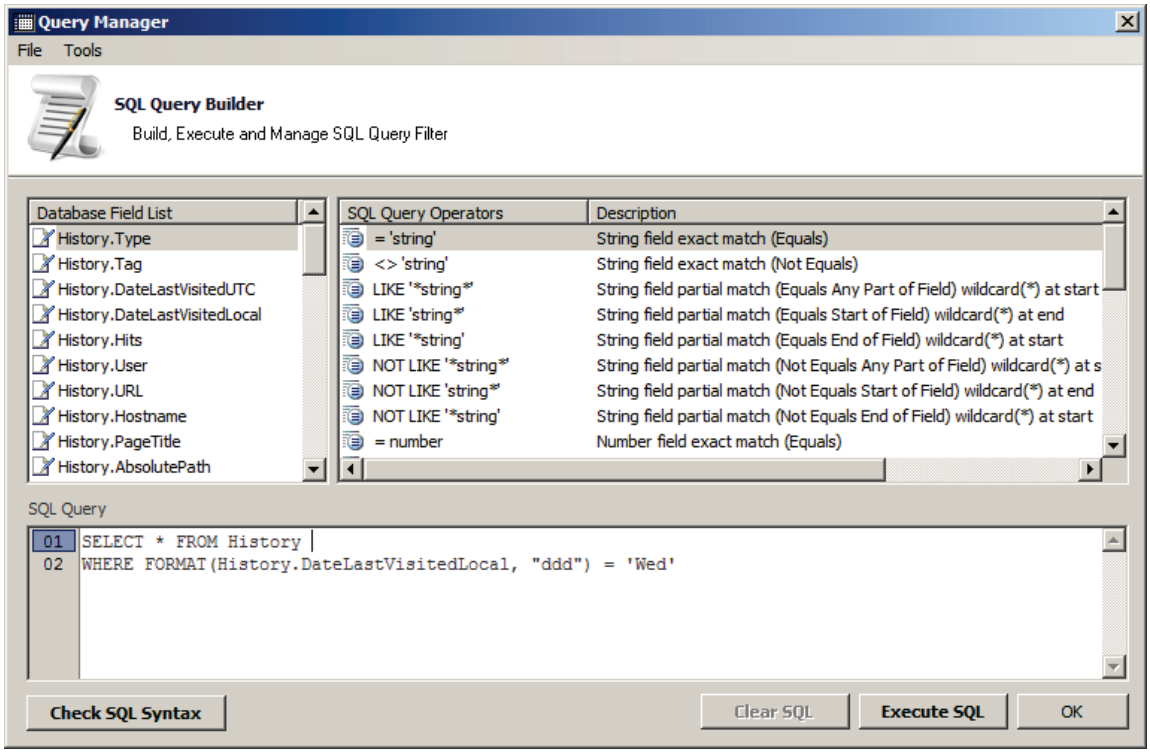


Figure 104

The SQL Query shown in Figure 104 will filter all history that took place on a Wednesday. To execute the query, select the 'Execute SQL' button from the Query Builder (you can also clear query results from here), or select Searching » Execute SQL Query from the menu.

NetAnalysis also comes with a number of example SQL Queries which can be opened from the File menu within the query builder form (see Figure 105).

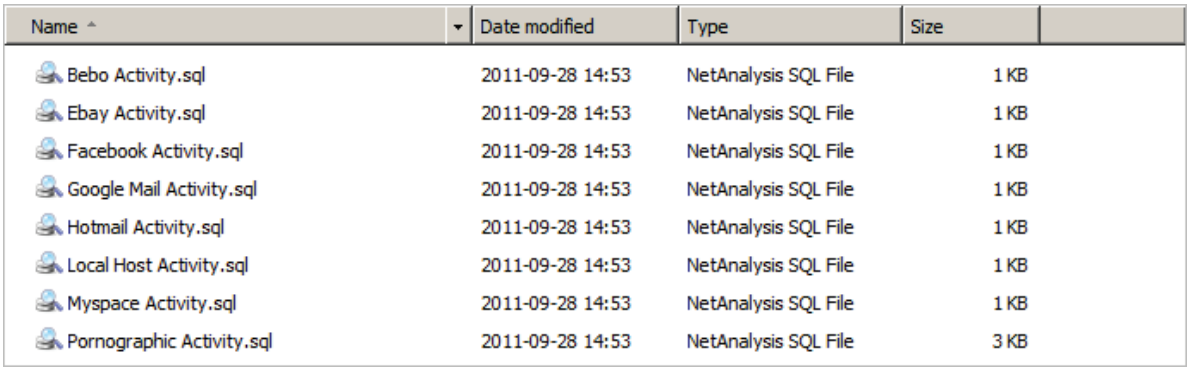


Figure 105

Sorting

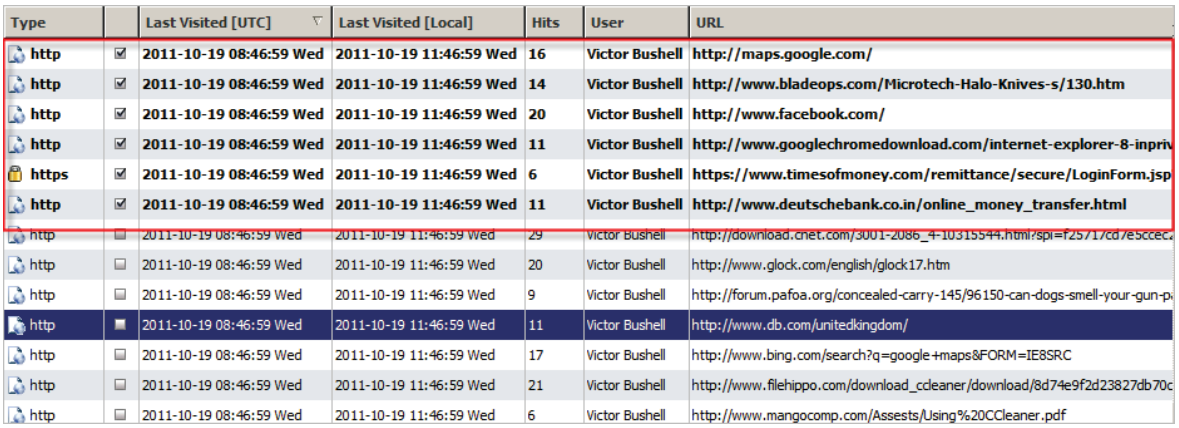
At any time, you can sort the order of the workspace records by clicking on the column header for the field you wish to order. The sort order can be toggled (ascending or descending) with subsequent clicks. The sort indicator is shown to the right of the column header (as shown in Figure 106). In this case, a descending sort is active.

Figure 106

If you wish to set a multiple level filter, or a multiple level sort, you will need to create a custom SQL query.

Tagging

When processing evidence and analysing browser records, you may wish to tag records of interest so that you can return quickly to them at a later point, or filter them. There are a couple of ways to tag a record. The quickest and most convenient is to press the space bar. The second method is to right click on the record and select Tag URL Record.



Type		Last Visited [UTC]	Last Visited [Local]	Hits	User	URL
http	☑	2011-10-19 08:46:59 Wed	2011-10-19 11:46:59 Wed	16	Victor Bushell	http://maps.google.com/
http	☑	2011-10-19 08:46:59 Wed	2011-10-19 11:46:59 Wed	14	Victor Bushell	http://www.bladeops.com/Microtech-Halo-Knives-s/130.htm
http	☑	2011-10-19 08:46:59 Wed	2011-10-19 11:46:59 Wed	20	Victor Bushell	http://www.facebook.com/
http	☑	2011-10-19 08:46:59 Wed	2011-10-19 11:46:59 Wed	11	Victor Bushell	http://www.googlechromedownload.com/internet-explorer-8-inpriv
https	☑	2011-10-19 08:46:59 Wed	2011-10-19 11:46:59 Wed	6	Victor Bushell	https://www.timesofmoney.com/remittance/secure/LoginForm.jsp
http	☑	2011-10-19 08:46:59 Wed	2011-10-19 11:46:59 Wed	11	Victor Bushell	http://www.deutschebank.co.in/online_money_transfer.html
http	☐	2011-10-19 08:46:59 Wed	2011-10-19 11:46:59 Wed	29	Victor Bushell	http://download.cnet.com/3001-2086_4-10315544.html?spi=f25717cd7e5cce
http	☐	2011-10-19 08:46:59 Wed	2011-10-19 11:46:59 Wed	20	Victor Bushell	http://www.glock.com/english/glock17.htm
http	☐	2011-10-19 08:46:59 Wed	2011-10-19 11:46:59 Wed	9	Victor Bushell	http://forum.pafoa.org/concealed-carry-145/96150-can-dogs-smell-your-gun-p
http	☐	2011-10-19 08:46:59 Wed	2011-10-19 11:46:59 Wed	11	Victor Bushell	http://www.db.com/unitedkingdom/
http	☐	2011-10-19 08:46:59 Wed	2011-10-19 11:46:59 Wed	17	Victor Bushell	http://www.bing.com/search?q=google+maps&FORM=IE8SRC
http	☐	2011-10-19 08:46:59 Wed	2011-10-19 11:46:59 Wed	21	Victor Bushell	http://www.filehippo.com/download_ccleaner/download/8d74e9f2d23827db70c
http	☐	2011-10-19 08:46:59 Wed	2011-10-19 11:46:59 Wed	6	Victor Bushell	http://www.mangocomp.com/Assests/Using%20CCleaner.pdf

Figure 107

Tagged records are changed to bold to make them easier to identify. When filtering tagged only records, the bold formatting is removed to make them easier to read.

Tags for the current filtered Recordset can be removed, or added, en masse by selecting Tools » Tag Current Filtered Records or Tools » Remove Tags from Current Filtered Records.

Moving Between Tagged Records

Sometimes you may wish to review the records on either side of a tagged record. This can easily be done by using the functionality to move between tagged records.

To find the next tagged record from your current position, select Searching » Find Next Tagged Record (F2) from the main menu. To find the previous tagged record from your current position, select Searching » Find Previous Tagged Record (Shift + F2) from the main menu.

Filtering Tagged Records

To filter and review tagged records, select Filter » Filter Tagged Records (F9).

Bookmarking

As you review and analyse the data, you may identify records which are of evidential value or relevant to the particular investigation. The bookmark field is set by the forensic examiner and contains a string which can be used to identify or describe a record.

The bookmark string appears in the Advanced Report and is commonly used to annotate particular records when they are of evidential value to your case. The Record Bookmark window (as shown in

Figure 108), can be activated by any of the following methods when the corresponding record is selected:

- Press the Enter Key;
- Right click and select Add/Edit Bookmark;
- Select Bookmark » Add/Edit Bookmark from the main menu.

In the text box at the bottom of the window, the forensic examiner can enter a free text description for the URL.

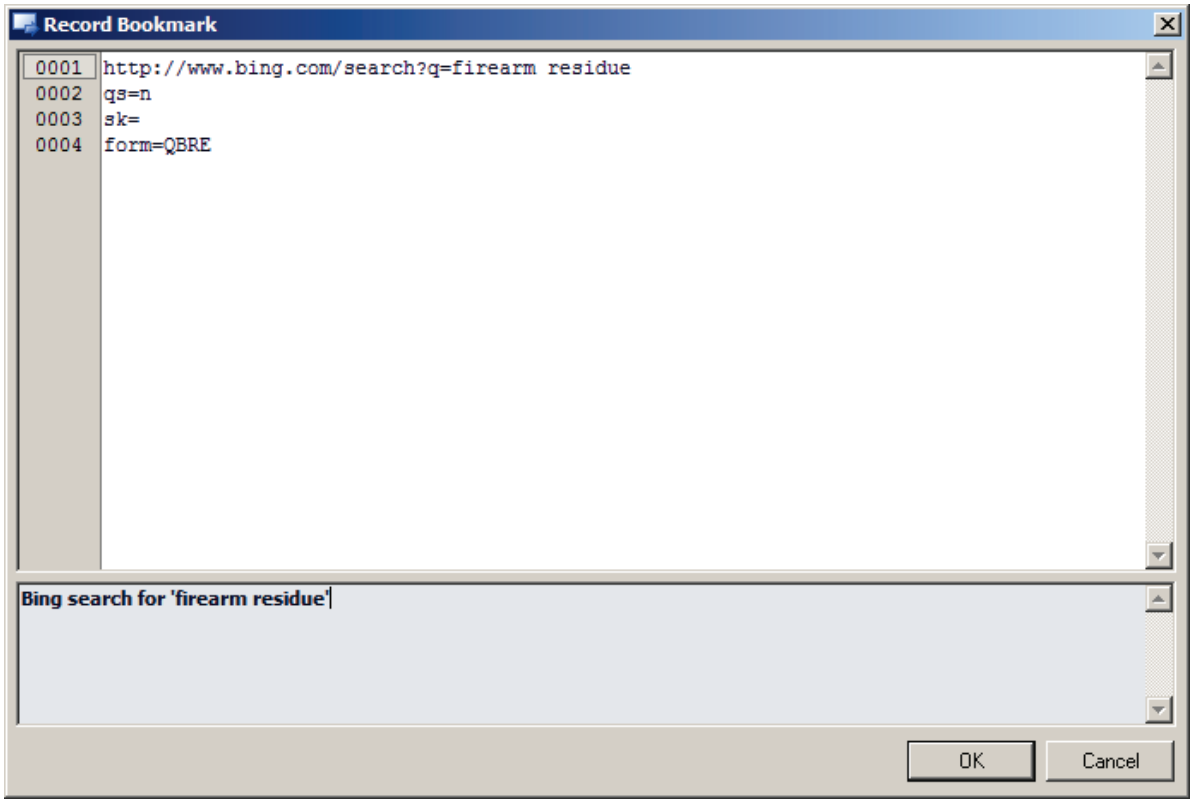
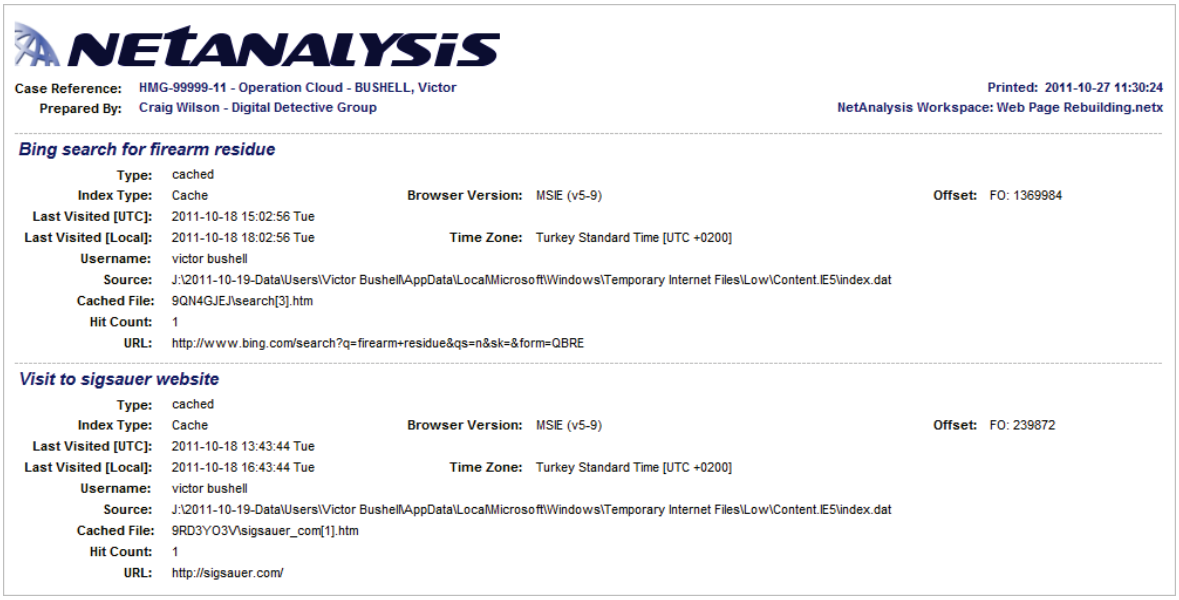


Figure 108

When the item has been bookmarked, the string text will appear in the bookmark column, as well as displaying a bookmark icon to the left of the URL (as shown in Figure 109). Bookmarked records can also be easily filtered by selecting Filter » Filter Records with Bookmarks

Figure 109

Figure 110 shows the bookmarked records displayed in the Advanced Evidence Report.



NETANALYSIS

Case Reference: HMG-99999-11 - Operation Cloud - BUSHELL, Victor
Prepared By: Craig Wilson - Digital Detective Group

Printed: 2011-10-27 11:30:24
NetAnalysis Workspace: Web Page Rebuilding.netx

Bing search for firearm residue

Type:	cached				
Index Type:	Cache	Browser Version:	MSIE (v5-9)	Offset:	FO: 1369984
Last Visited [UTC]:	2011-10-18 15:02:56 Tue				
Last Visited [Local]:	2011-10-18 18:02:56 Tue	Time Zone:	Turkey Standard Time [UTC +0200]		
Username:	victor bushell				
Source:	J:\2011-10-19-Data\Users\Victor Bushell\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\index.dat				
Cached File:	9QN4GJEJ\search[3].htm				
Hit Count:	1				
URL:	http://www.bing.com/search?q=firearm+residue&qs=n&sk=&form=QBRE				

Visit to sigsauer website

Type:	cached				
Index Type:	Cache	Browser Version:	MSIE (v5-9)	Offset:	FO: 239872
Last Visited [UTC]:	2011-10-18 13:43:44 Tue				
Last Visited [Local]:	2011-10-18 16:43:44 Tue	Time Zone:	Turkey Standard Time [UTC +0200]		
Username:	victor bushell				
Source:	J:\2011-10-19-Data\Users\Victor Bushell\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\index.dat				
Cached File:	9RD3YO3V\sigsauer_com[1].htm				
Hit Count:	1				
URL:	http://sigsauer.com/				

Figure 110

Right Click Context Menu

A number of the more common functions can be accessed by right clicking on a record to display the context menu (as shown in Figure 111).

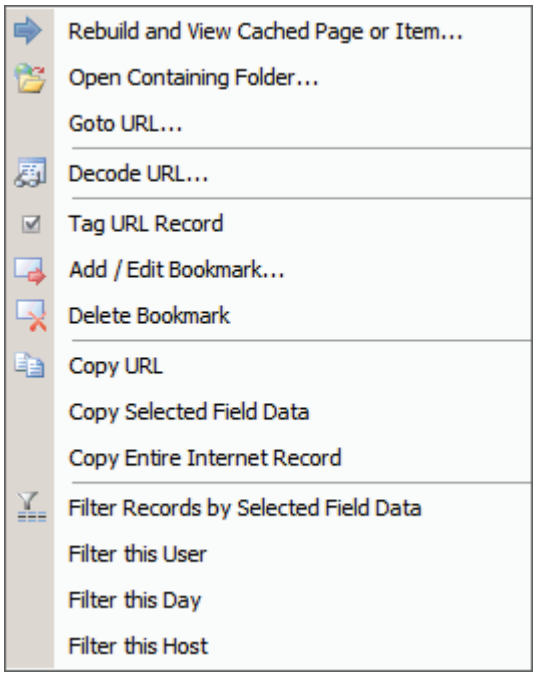


Figure 111

Table 25 contains a list of menu items and explains the function of each item.

Menu Item	Information
Rebuild and View Cached Page or Item	For a live cached item or page, this function will rebuild and show the cached web page, or cached item.
Open Containing Folder	For a live cached item or page, this function will open the original cache folder and highlight the cached file for the selected record.
Goto URL	This will launch the URL for the currently selected record in the default browser.
Decode URL	This will launch the Decode URL window and display a decoded version of the currently selected URL.
Tag URL Record	This will tag (or remove a tag if already set) the currently selected record.
Add / Edit Bookmark	The will launch the Bookmark window allowing a bookmark to be added to the currently selected record.
Delete Bookmark	This will remove the bookmark from the currently selected record.
Copy URL	This will copy the URL for the currently selected record to the clipboard.
Copy Selected Field Data	This will copy the data from the currently selected field/record to the clipboard.
Copy Entire Internet Record	This will copy each field for the visible columns, for the currently selected record, in a structured format, to the clipboard. This function can be used to copy record data into an external report.
Filter Records by Selected Field Data	This will filter the workspace using the data from the selected field for the currently selected record.
Filter this User	This will filter the workspace using the data from the user field for the currently selected record.
Filter this Day	This will filter the workspace for records for the 24 hour period of the currently selected record.
Filter this Host	This will filter the workspace for records relating to the currently selected host.

Table 25

Understanding the Evidence

Introduction

In this chapter, we look at understanding and interpreting URL data. A typical extraction can result in the forensic examiner having to review many thousands of records, so being able to quickly identify relevant evidence is very important.

URL

During our examination of browser artefacts, we will often be referring to URLs, or Uniform Resource Locators. In web terms, a resource represents anything available on the web, whether it is an HTML page, an image, a CGI script, etc. URLs provide a standard way to locate these resources on the World Wide Web. URLs are not specific to HTTP (Hypertext Transfer Protocol); they can refer to resources in many protocols. The following information refers to HTTP URLs.

HTTP URLs consist of a scheme, a host name, a port number, a path, a query string, and a fragment identifier, any of which may be omitted under certain circumstances.

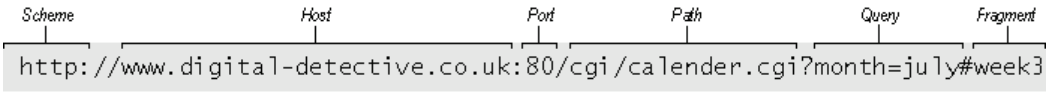


Figure 112

HTTP URLs contain the following elements:

Scheme

The scheme represents the protocol, and for our purposes will either be http, https or file. Https represents a connection to a secure web server (Secure Socket Layer).

Host

The host identifies the machine running a web server. It can be a domain name or an IP address.

Port number

The port field defines the protocol port used for contacting the server referenced in the URL. The port number is optional and may appear in URLs only if the host is also included. The host and port

are separated by a colon. If the port is not specified, port 80 is used for http URLs and port 443 is used for https URLs.

Path Information

Path information represents the location of the resource being requested, such as an HTML file or a CGI script. Depending on how the web server is configured, it may or may not map to some actual file path on the system.

Note that the URL for a script may include path information beyond the location of the script itself. For example, say you have a CGI at:

```
http://localhost/cgi/browse_docs.cgi
```

Figure 113

```
http://localhost/cgi/browse_docs.cgi/docs/product/description.txt
```

Figure 114

Here the path /docs/product/description.txt is passed to the script.

Query String

Query information is separated from the path information by a question mark (?) and continues to the end of the URL. The query information returned includes the leading question mark. A query string passes additional parameters to scripts. It is sometimes referred to as a search string or an index.

It may contain name and value pairs, in which each pair is separated from the next pair by an ampersand (&), and the name and value parts are separated from each other by an equals sign (=).

Query strings can also include data that is not formatted as name-value pairs. If a query string does not contain an equals sign, it is often referred to as an index (see Figure 115 for an example of a URL containing a query string).

```
http://www.google.co.uk/search?sourceid=chrome&ie=UTF-8&q=sslhostinfo
```

Figure 115

Fragment identifier

The Fragment field shows any text following a fragment marker (#) in the URL, including the fragment marker itself. Fragment identifiers refer to a specific section in a resource. Once the browser has fetched the resource it applies the fragment identifier to locate the appropriate section in the resource. For HTML documents, fragment identifiers refer to anchor tags within the document (as shown in Figure 116).

```
<a name="anchor">Here is the content you require...</a>
```

Figure 116

The following URL would request the full document and then scroll to the section marked by the anchor tag:

```
http://localhost/document.html#anchor
```

Figure 117

Absolute and Relative Paths

Many of the elements within a URL are optional. You may omit the scheme, host, and port number in a URL if the URL is used in a context where these elements can be assumed. For example, if you include a URL in a link on an HTML page and leave out these elements, the browser will assume the link applies to a resource on the same machine as the link.

There are two classes of URLs:

- Absolute URL;
- Relative URL.

Absolute URL

URLs that include the hostname are called absolute URLs. An example of an absolute URL is:

```
http://localhost/cgi/scripts/script.cgi
```

Figure 118

Relative URL

URLs without a scheme, host, or port are called relative URLs. These can be further broken down into full and relative paths:

- Full Paths;
- Relative Paths.

Full Paths

Relative URLs with an absolute path are sometimes referred to as full paths (even though they can also include a query string and fragment identifier). Full paths can be distinguished from URLs with relative paths because they always start with a forward slash. Note that in all these cases, the paths are virtual paths, and do not necessarily correspond to a path on the web server's file system. Examples of full paths include:

```
/index.html
/graphics/main.jpg
/test/graphics/example.png
```

Figure 119

Relative Paths

Relative URLs that begin with a character other than a forward slash are relative paths. Examples of relative paths include:

```
script.cgi
../images/picture.jpg
../../graphics/image.gif
```

Figure 120

URL Encoding

Many characters must be encoded within a URL for a variety of reasons. For example, certain characters such as question mark (?), hash or pound (#), and forward slash (/) have special meaning within URLs and will be misinterpreted unless encoded.

It is possible to name a file doc#5.html on some systems, but the URL http://localhost/doc#5.html would not point to this document. It would point to the fragment 5.html in a (possibly non-existent)

file named doc. We must encode the hash character (#) so the web browser and server recognise that it is part of the resource name instead.

Characters are encoded by representing them with a percent sign (%) followed by the two-digit hexadecimal value for that character based upon the ISO Latin 1 character set or ASCII character set (see the Extended ASCII Table on Page 155; these character sets are the same for the first eight bits). For example, the hash (#) symbol has a hexadecimal value of 0x23, so it is encoded as %23.

Table 26 contains a list of characters which must be encoded:

Character Type	Information
Control Characters	0x00 to 0x1F plus 0x7F
Eight-bit Characters	0x80 to 0xFF
Special Characters	; / ? : @ & = + $,
Characters often used to delimit	< > # % "
Unsafe Characters	{ } | \ ^ [ ] `
Space	+ or %20

Table 26

Table 27 contains a list of characters which are permitted:

Character Type	Information
Letters	Upper and lower case: A - Z a - z
Digits	0 - 9
Specific Characters	- _ . ! ~ * ' ( )

Table 27

It is actually permissible, and not uncommon, for any of the allowed characters to also be encoded by some software; therefore, any application that decodes a URL must decode every occurrence of a percentage sign followed by any two hexadecimal digits.

It is also possible to find other forms of encoding such as Base64. Base64 encoding can be helpful when dealing with lengthy information in an HTTP environment. For example, a database might use Base64 encoding to encode a large unique id (generally 128-bit UUIDs) into a string for use as an HTTP parameter in HTTP forms or HTTP GET URLs.

Also, many applications need to encode binary data in a way that is convenient for inclusion in URLs, including hidden web form fields. Base64 is a convenient encoding to render them in a compact way as well as making them relatively unreadable when trying to obscure the nature of data from the casual human observer.

Using standard Base64 in a URL requires encoding of (+), (/) and (=) characters into standard percent-encoded hexadecimal which makes the string unnecessarily longer.

For this reason, a modified Base64 for URL variant exists, where no padding '=' will be used, and the (+) and (/) characters of standard Base64 are respectively replaced by (-) and (_) so that using URL encoders/decoders are no longer necessary, and have no impact on the length of the encoded value. This leaves the same encoded form intact for use in relational databases, web forms, and object identifiers in general.

Here are some examples of standard and encoded URLs:

```
1. http://www.google.com
2. http://%77%77%77%2E%67%6F%6F%67%6C%65%2E%63%6F%6D
3. http://66.102.9.99
4. http://%36%36%2E%31%30%32%2E%39%2E%39%39
5. http://1113983331
6. http://%31%31%31%33%39%38%33%33%33%31
```

Figure 121

Example 1 (http://www.google.com)

This shows the standard representation of a URL and is not encoded.

Example 2 (http://%77%77%77%2E%67%6F%6F%67%6C%65%2E%63%6F%6D)

This is an encoded version of the standard URL in example 1. The %77 value represents the HEX value 0x77. When this is converted to an ASCII code (character code 119), we get the lowercase letter w. %2E represents the Hex value 0x2E. When this is converted to an ASCII code (character code 46), we get the period or full stop character.

Example 3 (http://66.102.9.99)

This example shows an IP address. Entering this into the browser address box will take you directly to a web page. The IP address can be further encoded.

Example 4 (http://%36%36%2E%31%30%32%2E%39%2E%39%39)

This is an encoded version of the IP address. As before, the %2E is translated to the Hex value 0x2E, which represents the ASCII code 46 which is a period or full stop. From the start of the

encoded URL, %36 represents the Hex value 0x36. Once again, translate this into the ASCII character code and you will get the number 6. This represents the first digit of the IP address. Continue the translation and you will get all the digits of the IP address.

Example 5 (http://1113983331)

To decode this example you must take the decimal value above and convert it to Hexadecimal. The Hex value is 0x42660963. Split this into 42 66 09 63 and convert back to decimal as follows: 0x42 = 66, 0x66 = 102, 0x09 = 9 and 0x63 = 99. This shows the IP address.

Example 6 (http://%31%31%31%33%39%38%33%33%33%31)

This is an encoded version of the data from Example 5. %31 represents the Hex value 0x31, which in turn represents the ASCII code 49. The ASCII character for 49 is the number 1.

Web Page Rebuilding

Overview

Rebuilding a web page from the data contained within a suspect's Temporary Internet Files (also known as the Cache) can be one of the strongest pieces of evidence available. NetAnalysis was the first forensic software to include the functionality for rebuilding web pages from an offline cache.

WARNING: Do not examine rebuilt web pages on a workstation which is connected to the Internet. Whilst every effort is made to disable links to external content, embedded scripting and code may result in requests being made for content from external servers when pages are viewed. This risk is negated by adhering to forensic best practice and not allowing forensic workstations to have live Internet connections.

To rebuild a cached page, you will need to have access to the live cache data. This can either be a cache exported from a forensic image, copied from a write protected suspect disk or from a mounted forensic image (see the warning in the section on Importing Cached Content from a Folder Structure).

Cached web pages can only be rebuilt successfully from a live cache. A live cache is one where the cached objects and corresponding cache database records are still available and have not been deleted.

Although we can recover deleted cache records, it is not possible to rebuild web pages without all the objects being present.

Practice Files

In our Bushell scenario (see the section on Practice Files on Page 49), the data zip archive contains exported browser INDEX records and cached content. It is this data we will use in the following example.

Importing Cached Content from a Folder Structure

To import the cache records, we will use the 'Open All History from Folder' method. This option will recursively search the file system for supported files and then import any that have been found.

WARNING: Some third party image mounting tools do not deal with NTFS symbolic links correctly within a forensic environment. Testing has identified an issue where NTFS symbolic links on mounted volumes point to folders on the forensic examiners own hard disk. See knowledge base article: KB80018.

To access the recursive import, select File » Open All History from Folder (as shown in Figure 122).

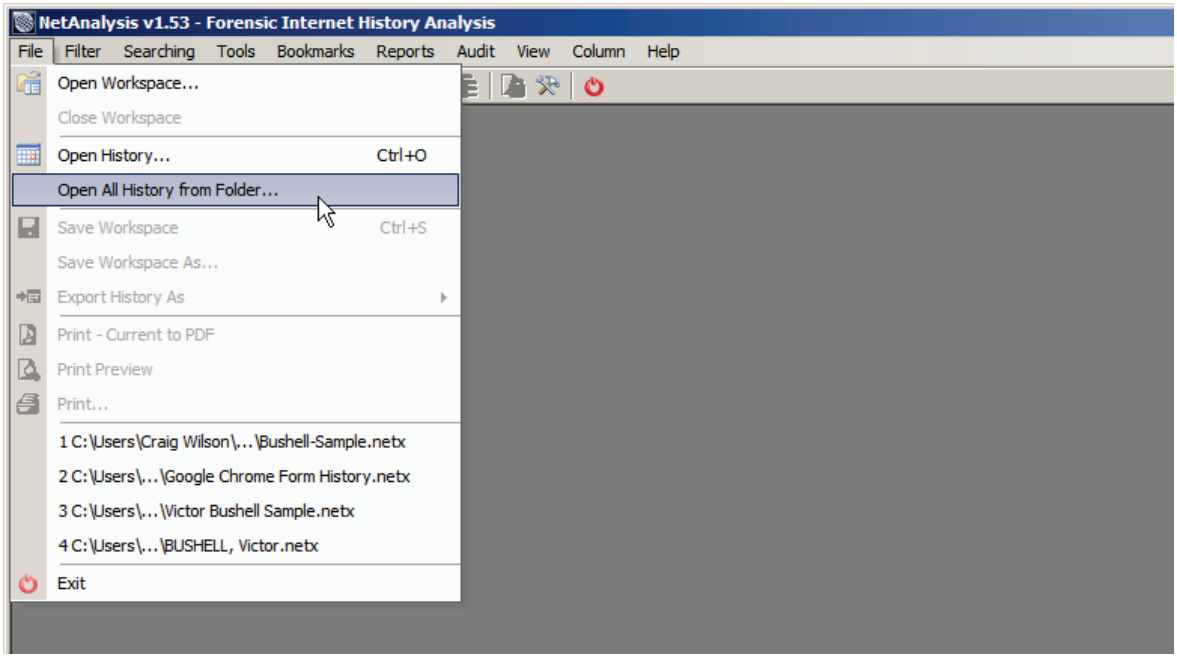


Figure 122

The Browse for Folder window will then open. Navigate to the drive containing your Victor Bushell data, and select the folder containing the user profile (see Figure 123).

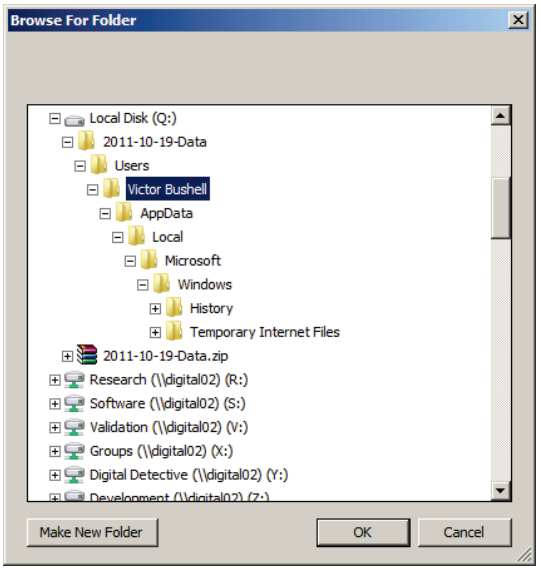


Figure 123

Click OK to start searching through the profile for supported browser files. NetAnalysis should identify 16 possible browser files from this data.

Once each file has been identified, NetAnalysis will start to import each record into the temporary workspace. The progress will be displayed as shown in Figure 124.

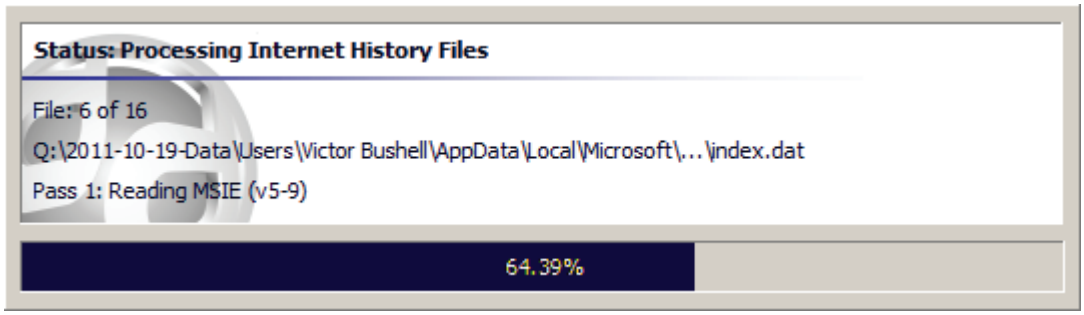


Figure 124

Once the records have been imported, NetAnalysis will display the summary screen as shown in Figure 125. This window shows that all the records have been imported successfully. It shows that 16 files have been imported with a total of 10,509 records identified.

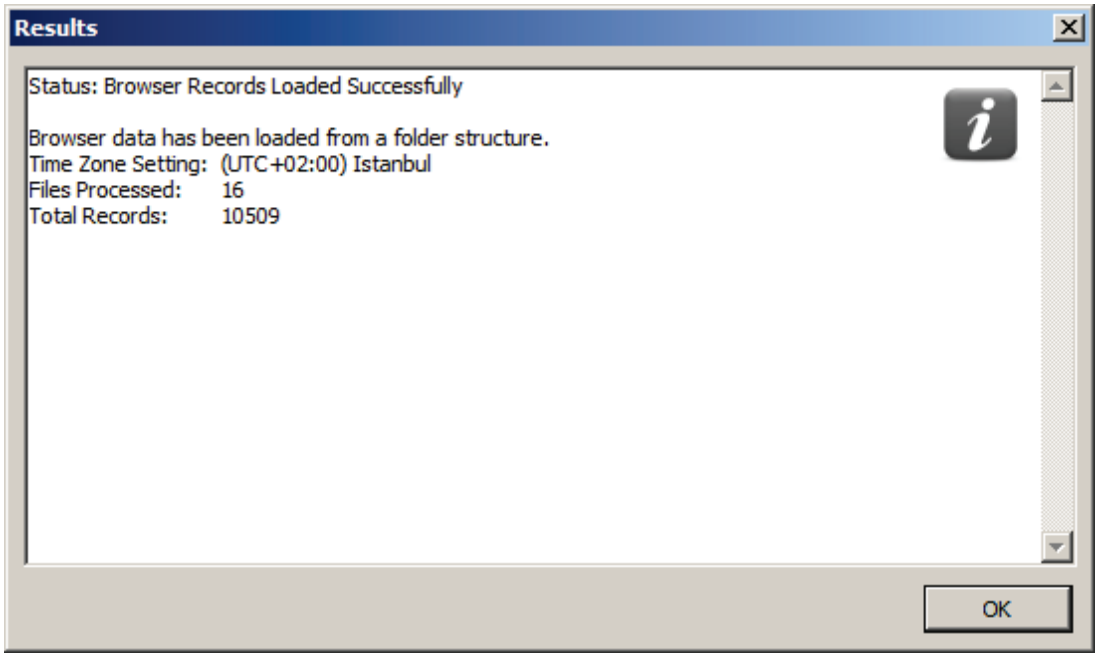


Figure 125

The window also shows that the time zone settings for this import was '(UTC +0200) Istanbul', which is the time zone we set prior to importing any data. This information is also written to the audit log.

You should now have a NetAnalysis window similar to Figure 126 with a total of 10,509 records imported into the workspace.

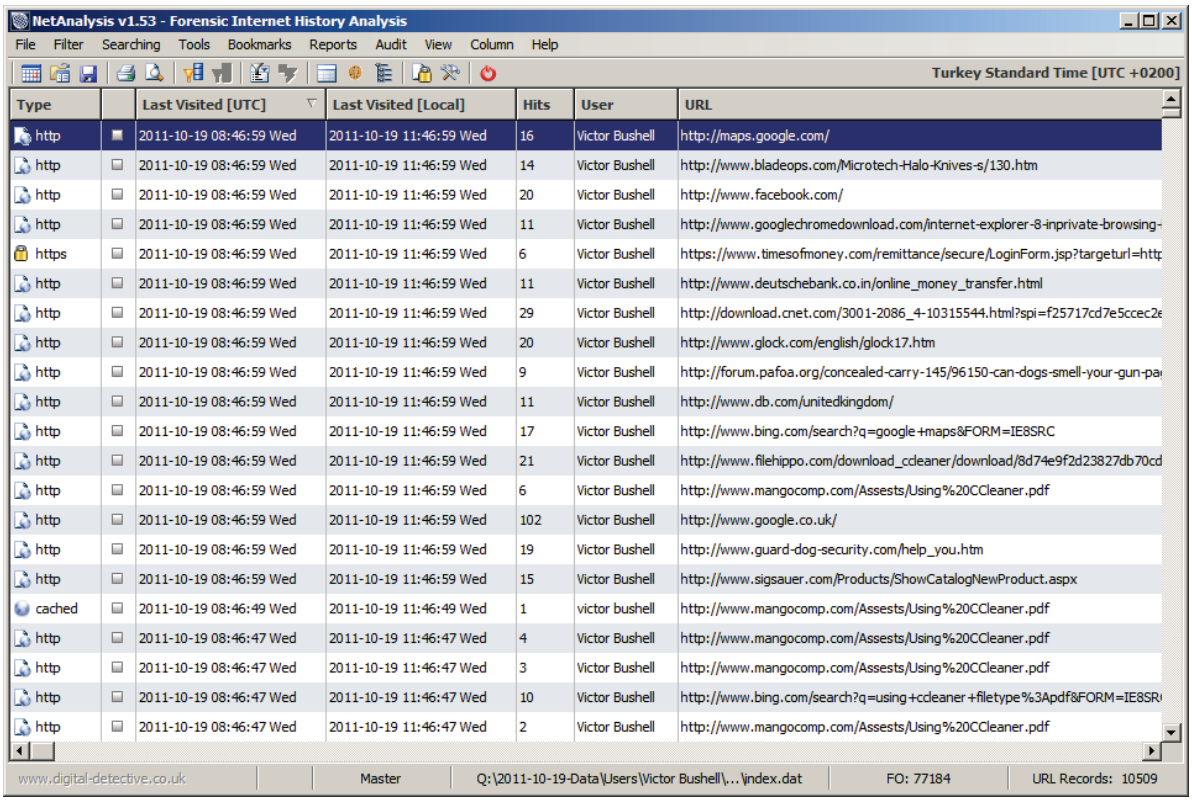


Figure 126

Save the workspace if you have not already done so.

Filtering Cached Items

To view the cached items from the workspace, select Filter » Cache Record Types » Cached Files Type from the menu (as shown in Figure 127).

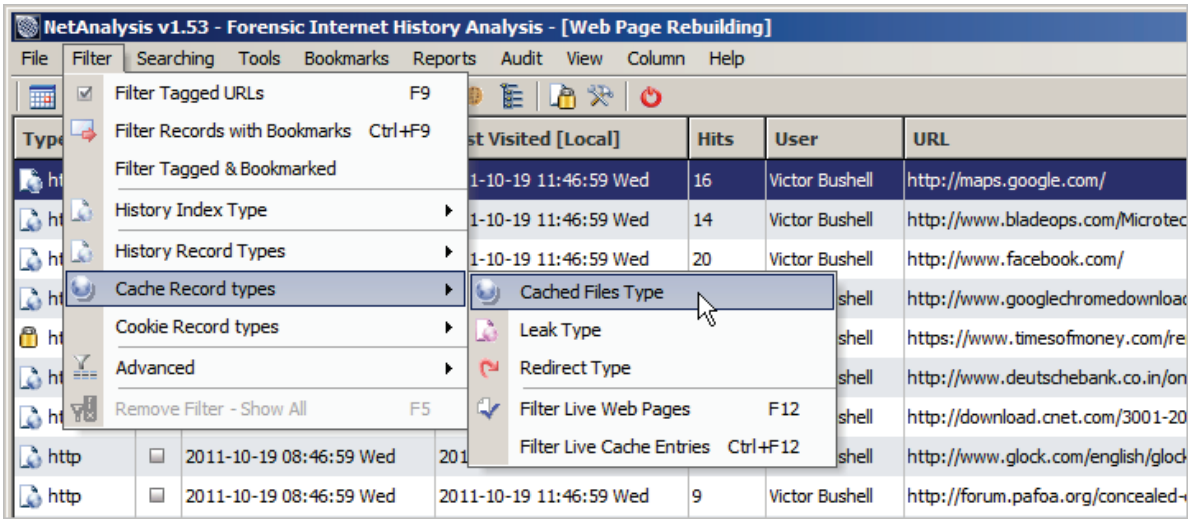


Figure 127

Figure 128 shows a typical cached entry; this particular entry relates to a PNG file. The Cache Folder column shows the folder the cached item has been saved to. The Cache File column shows the name Internet Explorer has assigned that particular cached item. The Exists column shows that the item is live and can be viewed or used as part of the web page rebuilding process. You will not be able to view any items which do not exist in the cache.

Type	URL	Cache Folder	Cache File	Exists
cached	http://www.bing.com/fd/s/a/sw3.png	9RD3YO3V	sw3[1].png	

Figure 128

The Source File which holds the cached records is shown in Figure 129.

Source File
J:\2011-10-19-Data\Users\Victor Bushell\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\index.dat

Figure 129

To view this cached item in its original location, right click on the record and select Open Containing Folder from the context menu. This will open the cache folder and highlight the cached item (as shown in Figure 130).

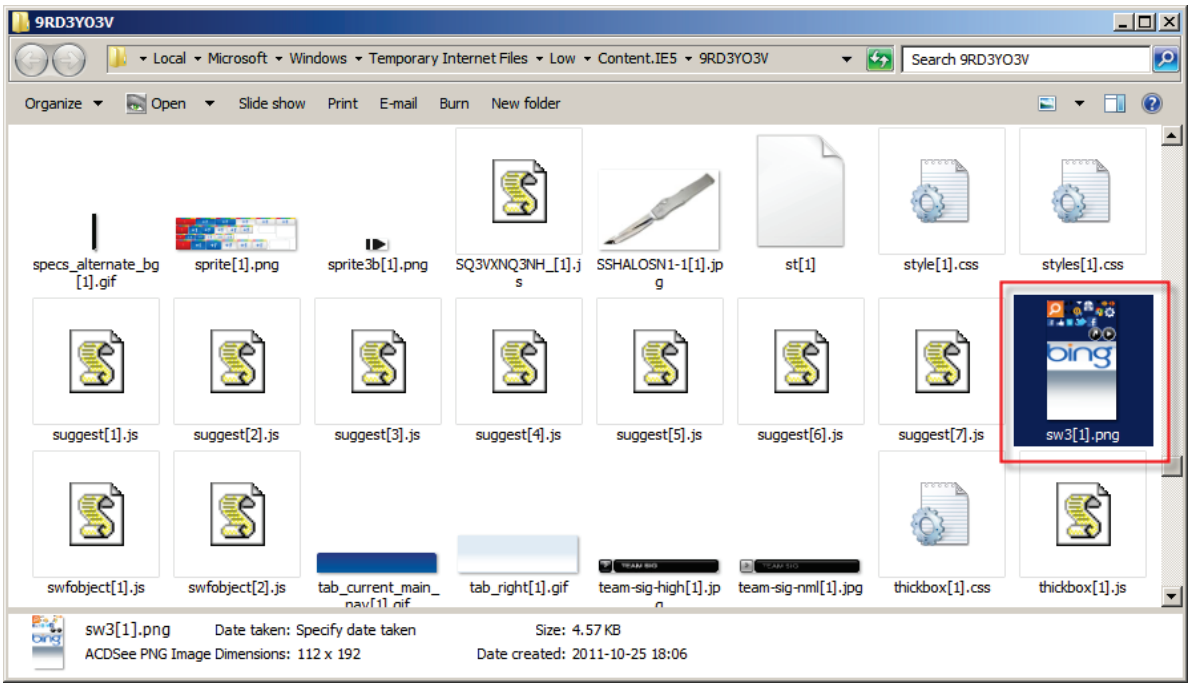


Figure 130

To view the cached item in the built-in viewer, either double click the record, or select Rebuild and View Cached Page or Item from the right click context menu.

At this point, as we have only just imported this cached data, we have not set an export folder for cached items to be saved to. NetAnalysis will prompt us to set an export folder at this point (see Figure 131).

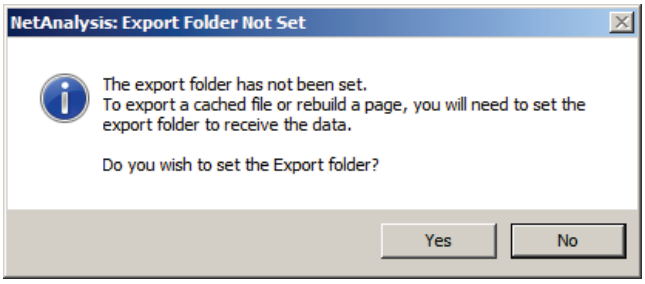


Figure 131

When you click 'Yes', the Options window will open with the Case Data Paths panel selected allowing you to enter an export folder (as shown in Figure 132). Once the export folder has been set, NetAnalysis will use this location to store exported items and rebuilt web pages.

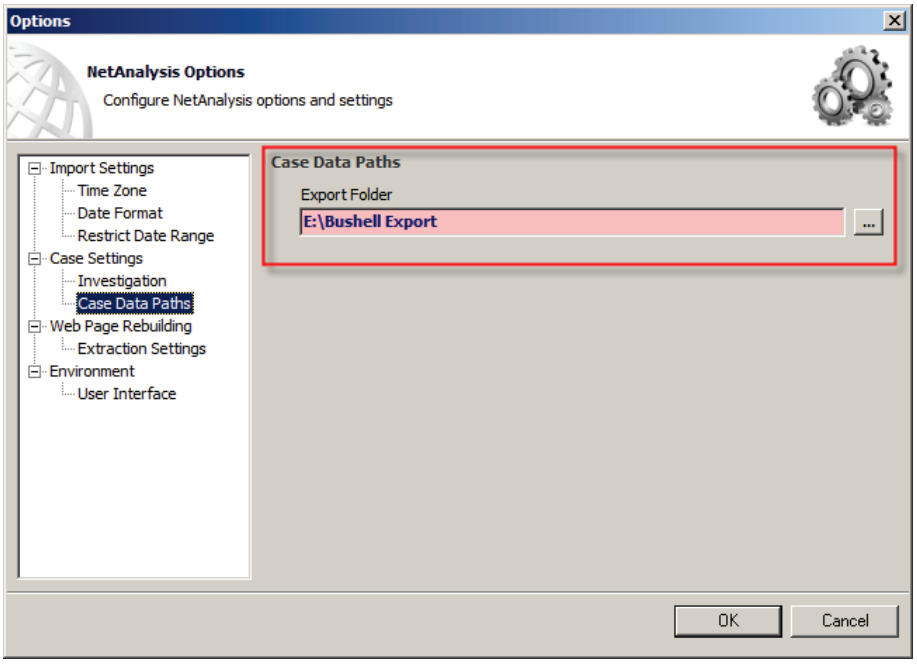


Figure 132

Now the export folder has been set, click OK. NetAnalysis will copy the cached item to the export folder and launch it in QDV, the internal file and page viewer (as shown in Figure 133).

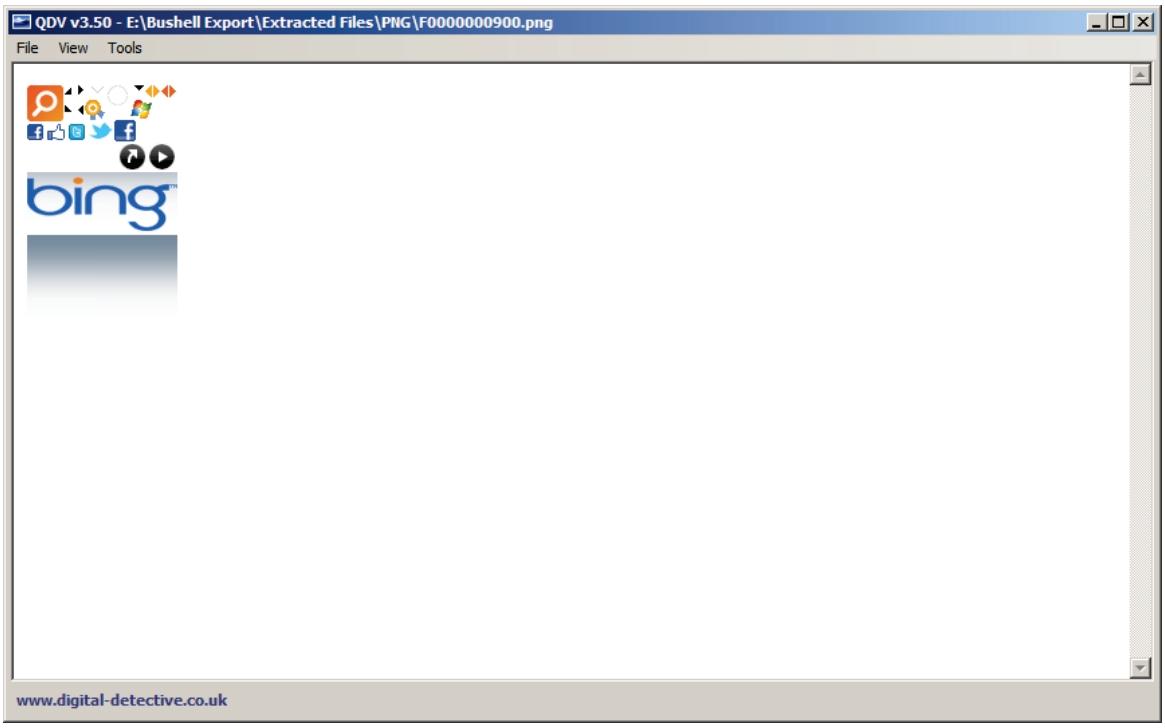


Figure 133

If you had set the 'Use Default File Viewer' option in the Extraction Settings, NetAnalysis would have launched the default file viewer for PNG files on your system. This option can be set by selecting Tools » Options » Web Page Rebuilding » Extraction Settings (as shown in Figure 134).

Figure 134

There is a further option to Group Output Files by Extension. This option is activated by default (see Figure 135).

Figure 135

When this option is set, the exported cached item is copied to a folder that matches the items file extension.

When the PNG file was double clicked and viewed, it was first extracted from the cache and copied to the export folder. If we look at the export folder we can see the item has been copied (and renamed) to a folder called PNG (see Figure 136).

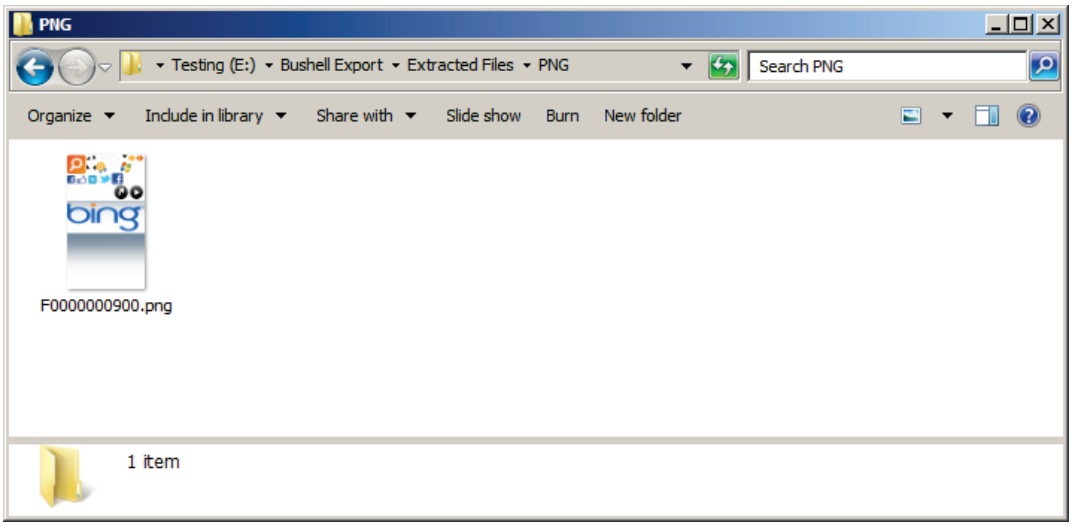


Figure 136

As there is a possibility we may have a filename collision with exported cached items, NetAnalysis renames each item according to the URN (Unique Reference Number) in the workspace.

Type	URL	Cache Folder	Cache File	Exists	URN
cached	http://www.bing.com/fd/s/a/sw3.png	9RD3YO3V	sw3[1].png	✓	900

Figure 137

To match an exported item with a cache record, match the number in the filename with the URN of the record (as shown in Figure 137).

Rebuilding an Individual Web Page

The process for rebuilding an entire web page is the same as for viewing a single cached item. To filter the live cached web pages, select Filter » Cache Record Types » Filter Live Web Pages.

To rebuild a web page, select the record for a cached page and then double click the record. Alternatively, select Rebuild and View Cached Page or Item from the right click context menu.

Figure 138 shows a rebuilt web page where the Default File Viewer option was set. This page relates to record URN 3046 from the workspace.

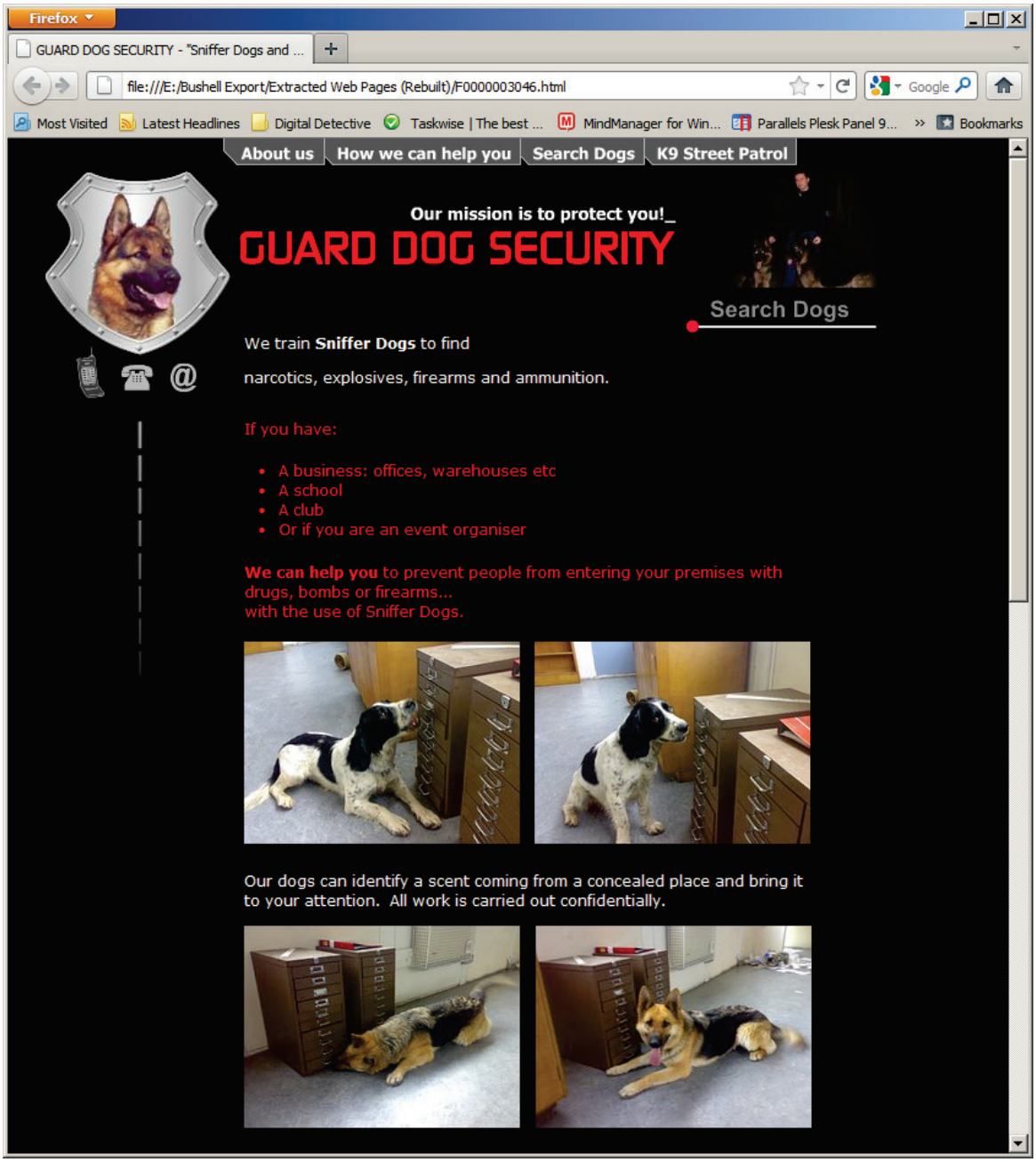


Figure 138

How Does NetAnalysis Rebuild a Web Page

In simple terms, to view a web page in its original state, a number of changes must be made to the internal HTML code. To get the page to function off-line, paths to all of the cached elements must be updated to point to their new saved location.

For stage 1, all of the cached page elements are identified. For stage 2, the workspace is searched to identify all the corresponding cache records for that page. For stage 3, the location of each cached item is identified. For stage 4, each cached item is exported and copied to a dedicated

folder specifically for that cached page. For stage 5, the page is edited in memory and the pointers for each cached item are updated to point to the exported location. When the rebuilt web page is saved to the export location, it is then launched for viewing. Figure 139 outlined the 5 steps required to complete the process.

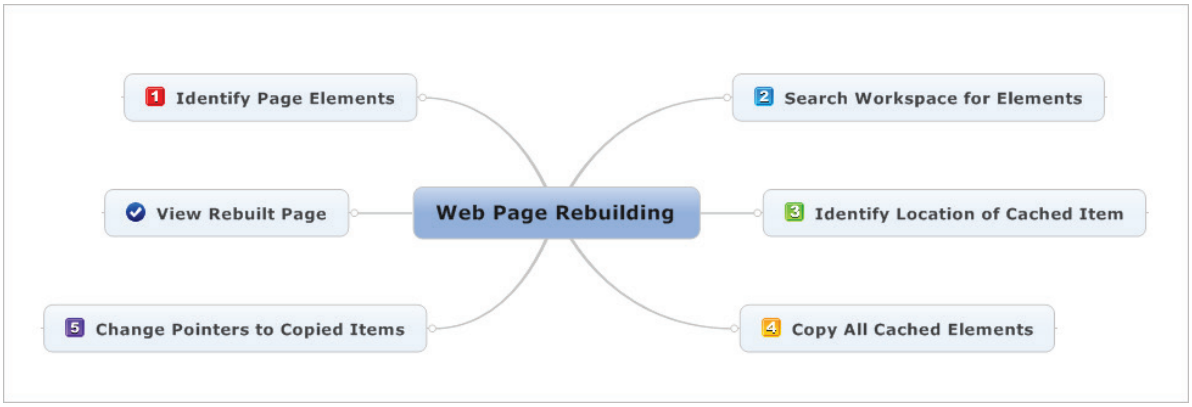


Figure 139

Rebuild Audit

As each web page is rebuilt (as outlined in Figure 139), NetAnalysis creates an audit log of the entire process. Each HTML audit log is saved to the export folder in a folder called Audit Pages.

NETANALYSIS

NetAnalysis - Page Rebuild Audit Log

Version:	NetAnalysis v1.53 (1.53.11280.253)
Licenced User:	Digital Detective Group
Licence ID:	0xFA85FB4C
Case Reference:	HMG-99999-11
Suspect/Operation:	Operation Cloud - BUSHELL, Victor
Forensic Examiner:	Craig Wilson
Agency/Company:	Digital Detective Group

Source File	J:\2011-10-19-Data\Users\Victor Bushell\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\index.dat
Source Offset	FO: 1351936
Browser Version	MSIE (v5-9)
Source URL	http://www.guard-dog-security.com/search_dogs.htm
Cache File	TD06QBFX\search_dogs[1].htm
Output File	F0000003046.html
Last Visited [UTC]	2011-10-18 14:59:04
Last Visited [Local]	2011-10-18 17:59:04
Date Last Synch [UTC]	2011-10-18 14:59:06
Rebuild Date	2011-10-26 13:00:34.825

Figure 140

Figure 140 shows the top section of an Audit Log. This section includes information relating to the software and licenced user. It also includes information relating to the source page. The output file field contains a hyperlink which can be clicked to launch the exported, rebuilt web page.

The second section of the log (as shown in Figure 141) shows a table containing the original URL from the original page, the corresponding cache file and the associated output file. The output file contains a hyperlink which can be clicked to view the exported cached item.

Original URL	Cache File	Output File
http://www.guard-dog-security.com/img/but_about_1.gif	9RD3YO3V\but_about_1[1].gif	F0000003046_Files\F0000003062.gif
http://www.guard-dog-security.com/img/but_what_1.gif	TD06QBFX\but_what_1[2].gif	F0000003046_Files\F0000003038.gif
http://www.guard-dog-security.com/img/but_search_1.gif	TD06QBFX\but_search_1[2].gif	F0000003046_Files\F0000003039.gif
http://www.guard-dog-security.com/img/but_k9_1.gif	TD06QBFX\but_k9_1[1].gif	F0000003046_Files\F0000003041.gif
http://www.guard-dog-security.com/img/top_new.swf	9RD3YO3V\top_new[1].swf	F0000003046_Files\F0000003053.swf
http://www.guard-dog-security.com/img/logo_new.swf	9RD3YO3V\logo_new[1].swf	F0000003046_Files\F0000003054.swf
http://www.guard-dog-security.com/img/name_Search%20Dogs.gif	TD06QBFX\name_Search%20Dogs[1].gif	F0000003046_Files\F0000003044.gif
http://www.guard-dog-security.com/img/Oscar%20at%20work_1.jpg	9QN4GJEJ\Oscar%20at%20work_1[1].jpg	F0000003046_Files\F0000003049.jpg
http://www.guard-dog-security.com/img/Oscar%20at%20work_2.jpg	9RD3YO3V\Oscar%20at%20work_2[1].jpg	F0000003046_Files\F0000003050.jpg
http://www.guard-dog-security.com/img/At%20work_1.jpg	9QN4GJEJ\At%20work_1[1].jpg	F0000003046_Files\F0000003051.jpg
http://www.guard-dog-security.com/img/At%20work_2.jpg	TD06QBFX\At%20work_2[1].jpg	F0000003046_Files\F0000003045.jpg
http://www.guard-dog-security.com/img/line.swf	9RD3YO3V\line[1].swf	F0000003046_Files\F0000003052.swf
http://www.guard-dog-security.com/img/bottom_new.swf	PGQ57MZE\bottom_new[1].swf	F0000003046_Files\F0000003056.swf
http://www.guard-dog-security.com/img/_transp.gif	9QN4GJEJ_transp[2].gif	F0000003046_Files\F0000003061.gif
http://www.guard-dog-security.com/img/BIPDT_2.jpg	9QN4GJEJ\BIPDT_2[1].jpg	F0000003046_Files\F0000003043.jpg
http://www.guard-dog-security.com/img/_transp.gif	9QN4GJEJ_transp[2].gif	F0000003046_Files\F0000003061.gif
http://www.guard-dog-security.com/img/ukcpa_2.png	PGQ57MZE\ukcpa_2[2].png	F0000003046_Files\F0000003059.png
http://www.guard-dog-security.com/img/_transp.gif	9QN4GJEJ_transp[2].gif	F0000003046_Files\F0000003061.gif
http://www.guard-dog-security.com/img/NASDU_2.gif	PGQ57MZE\NASDU_2[1].gif	F0000003046_Files\F0000003055.gif
http://www.guard-dog-security.com/img/_transp.gif	9QN4GJEJ_transp[2].gif	F0000003046_Files\F0000003061.gif
http://www.google-analytics.com/urchin.js	9QN4GJEJ\urchin[2].js	F0000003046_Files\F0000003047.js
http://www.guard-dog-security.com/box.css	PGQ57MZE\box[1].css	F0000003046_Files\F0000003065.css

Figure 141

Rebuild and Export All Cached Items

NetAnalysis also has a feature to rebuild all live web pages and to export all live cached items. This process can be activated by selecting Tools » Export/Rebuild All Cached Items.

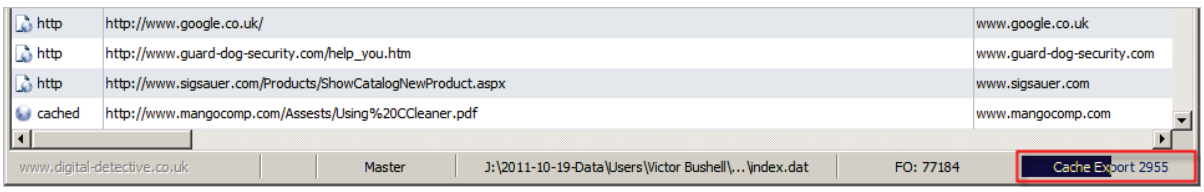


Figure 142

Figure 142 shows NetAnalysis exporting and rebuilding an entire cache. The progress is displayed in the bottom right hand corner of the status bar.

When NetAnalysis has completed the export, the Results window will be displayed (as shown in Figure 143).

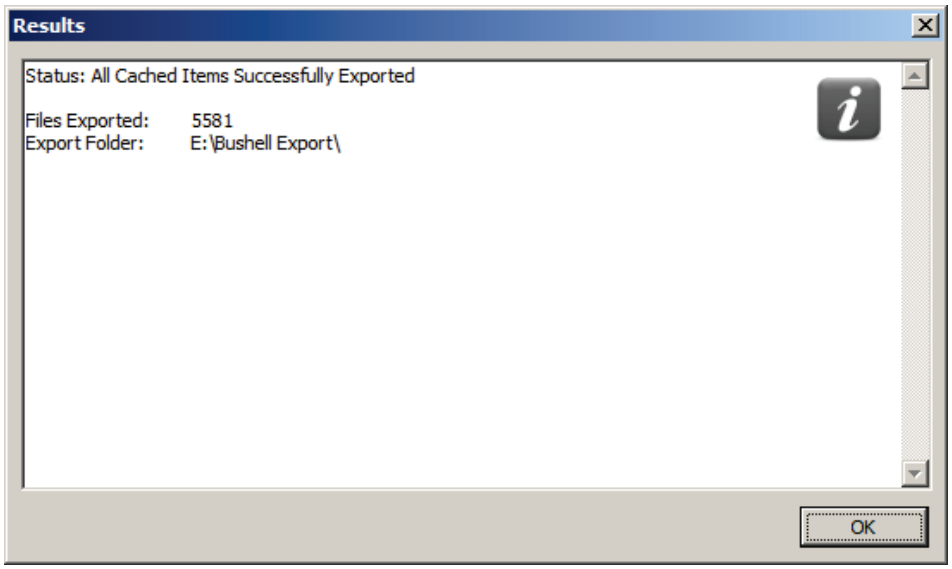


Figure 143

Some pages may contain hundreds of elements. As a result, they may take a few minutes to rebuild and export. Please be patient during the rebuild process. At times, it may appear as if the application has stopped responding.

Reporting

Introduction

There are a number of built-in reports available to the forensic examiner within NetAnalysis. Each report can be previewed on screen, sent to a printer or saved as a PDF file. Table 28 outlines each available report.

Report Name	Information
Simple Report	File » Print, File » Print Preview or File » Print - Current to PDF Prints the current filtered records: Type, Last Visited (Local), User, Hits and URL.
Group by Host	Reports » Group Reports » Group by Host Prints the current filtered records: Type, Last Visited (Local), User, and URL all grouped by the Host field.
Group by History File	Reports » Group Reports » Group by History File Prints the current filtered records: Type, Last Visited (Local), User, and URL all grouped by the Source File field.
Group by Index Type	Reports » Group Reports » Group by Index Type Prints the current filtered records: Type, Last Visited (Local), User, and URL all grouped by the Index Type field.
Group by User	Reports » Group Reports » Group by User Prints the current filtered records: Type, Last Visited (Local) and URL all grouped by the User field.
Total Entry Frequency Summary by Host	Reports » Total Entry Frequency Summary by Host Prints a summary report based on the count of each unique host within the entire workspace
Advanced Evidence Report	Reports » Advanced Evidence Report Prints a detailed summary of each filtered record showing the bookmark for each record.

Table 28

Advanced Report

The advanced report is one of the most useful reports, as it includes all the information you need to evidence a URL record.

Figure 144 shows the Advanced Report with two bookmarked records displayed.

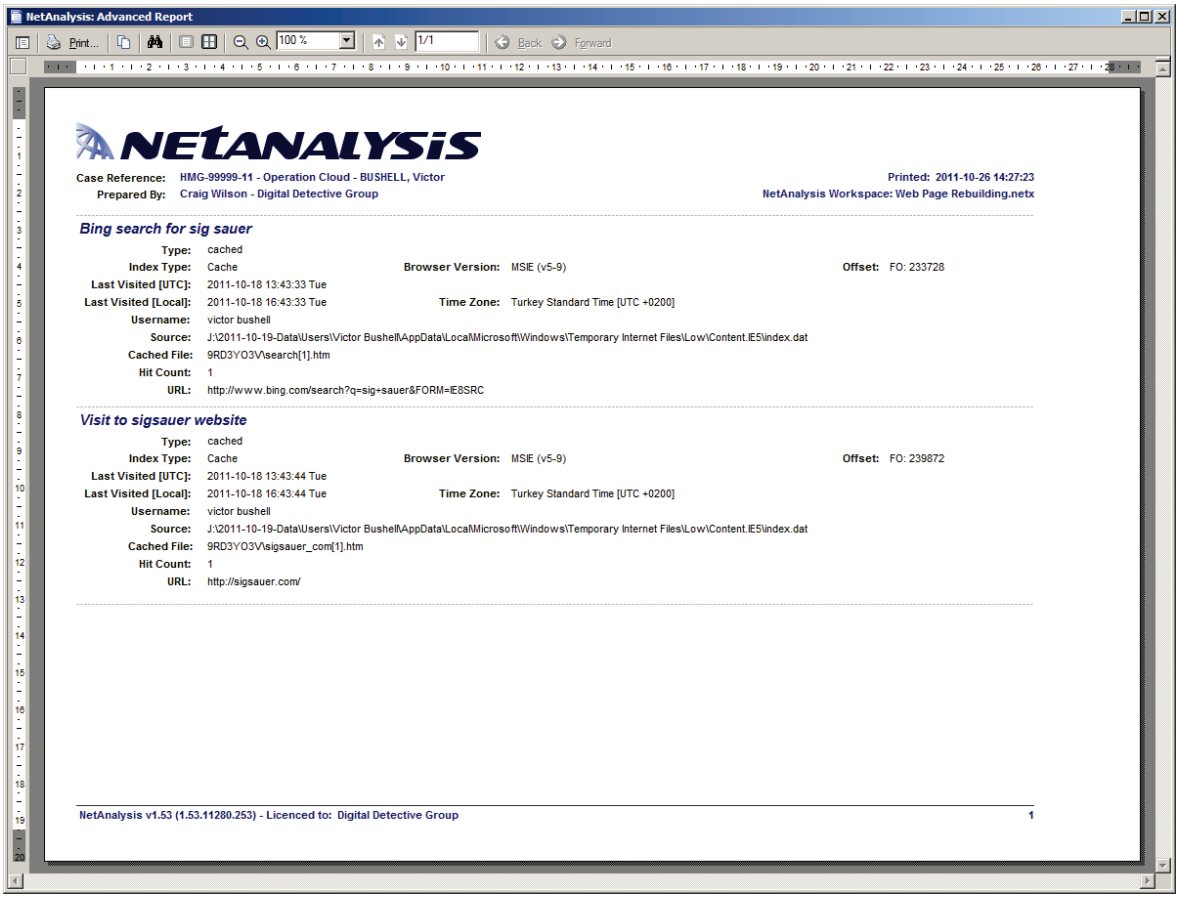
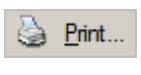


Figure 144

The report viewer has its own toolbar (as shown in Figure 145).

Figure 145

Table 29 explains the function of each button on the report viewer toolbar.

Button	Information
	Table of Contents Shows/Hides the Table of Contents pane
	Print Prints the current report and allows the selection of a printer
	Copy Copies the current page to the clipboard.

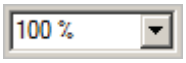
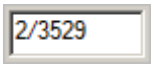
Button	Information
	Find Opens the find window and allows you to search through the report
	Single Page Resizes the report so that a single page is shown on screen
	Multiple Pages Resizes the report so that multiple pages are shown on screen
	Zoom Out Changes the zoom factor by zooming out
	Zoom In Changes the zoom factor by zooming in
	Zoom Percentage Changes the zoom factor for the current report
	Previous Page Moves the report on to the previous page
	Next Page Moves the report on to the next page
	Page X of Y Allows the user to jump to a specific page in the report
	Back Allows the user to move to the previously viewed report page
	Forward Allows the user to move forward after moving back

Table 29

Exporting

Introduction

Exporting data from NetAnalysis is a relatively easy process. Table 30 outlines the current export options.

Type	Scope	Information
TSV	Filtered Records / Visible Columns	Tab Separated Values
CSV	Filtered Records / Visible Columns	Comma Separated Values
HTML	Filtered Records / Visible Columns	HTML formatted document
PDF	Filtered Records	Via Reports (see Reporting on Page 132)
Database	Entire Workspace	Microsoft JET RED database (can be opened in Microsoft Access)

Table 30

Exporting to TSV

The TSV export can export the entire Recordset from the workspace, or a subset of filtered records. There is a further option to stipulate which fields are exported by hiding or displaying a column. Column visibility can be toggled by selecting or un-selecting a named column from the column menu. To export the data in TSV format, select File » Export History As » Tab Separated Values from the menu.

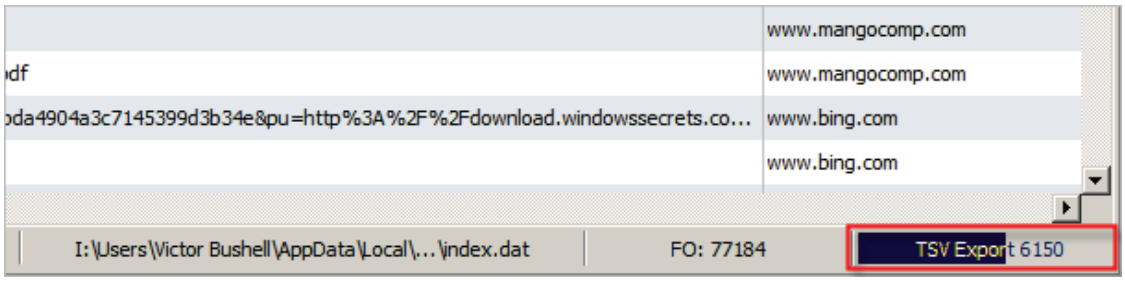


Figure 146

As the data is exported, NetAnalysis will show a progress bar in the bottom right of the status bar. If you wish to cancel the export, simply double-click on the progress bar.

When the export has completed, NetAnalysis will open the export folder and highlight the exported file.

Exporting to CSV

The process for exporting to CSV is exactly the same as for Tab Separated Values. To export the data in CSV format, select File » Export History As » Comma Separated Values from the menu.

Exporting to HTML

The process for exporting to HTML is exactly the same process as for TSV and CSV. To export the data in HTML document format, select File » Export History As » HTML File from the menu.

Exporting to PDF

The built-in reports can be exported in PDF format. For further information, please see the Chapter on Reporting on Page 132.

Exporting to a Database

The entire workspace can be exported to a Microsoft JET Red database (which can be opened in Microsoft Access). To export the workspace, select File » Export History As » MS Access Database from the menu.

Deleted Data Recovery

Introduction

A critical element of web browser forensic analysis is the recovery of deleted data. HstEx is an advanced, professional forensic data recovery solution, designed to recover browser artefacts and Internet history from a number of different source evidence types.

HstEx Processing

HstEx has been designed to process a forensic image, physical/logical disk or binary dump at sector level. It does not work at the file system level. The recovered data fragments are written out to a HSTX file which can then be imported into NetAnalysis.

When HstEx searches your source, it will search it a sector (or number of sectors depending on the block size set) at a time. HstEx uses linear processing and will examine each block of data contiguously. This means that it will potentially recover data from the areas outlined in Table 31.

Potential Evidence Source			
Unallocated Clusters	Allocated Clusters	Cluster Slack	Volume Slack
Memory Dumps	Binary Dumps	Swap Files	Hibernation Files
Unused Disk Space	Live Files	Resident Files	Deleted Files
Restore Points	Shadow Volumes	Hidden Partitions	Deleted Partitions

Table 31

HstEx works in a similar way to an imager in that it starts at sector zero and processes all the data to the end. In many cases, it can recover individual records relating to browser activity without the entire file being present on the source image or disk.

As HstEx ignores the file system, it can be run across many source file system types without issue. It also means that when it recovers from a disk or image, it will potentially recover the live data as well as any that is deleted.

To identify the location of source evidence, HstEx embeds the exact location of each data fragment inside the HSTX file. NetAnalysis can interpret the exact location and present that to the forensic

examiner. This allows an independent third party to verify the exact source of the evidence on the original source disk or image.

In addition to physical devices and volumes, HstEx supports all of the major forensic image formats (as shown in Table 32).

Forensic Image Source Type	Extension
EnCase® v1-7 Image File (EVF / Expert Witness Format)	*.e01
AccessData® FTK Image Files	*.e01, *.001, *.s01
SMART/Expert Witness Image File	*.s01
X-Ways Forensics Image File	*.e01
Tableau Imager	*.e01, *.dd
VMWare Virtual Disk File	*.vmdk
Virtual Hard Disk File	*.vhd
Segmented Image Unix / Linux DD / Raw Image Files	*.000, *.001
Single Image Unix / Linux DD/Raw Image Files	*.dd; *.img; *.ima; *.raw
Memory Dumps	*.dmp; *.dump; *.crash; *.mem; *.vmem; *.mdmp
Binary Dumps	*.bin; *.dat; *.unallocated; *.rec; *.data; *.binary
Micro Systemation Extraction File	*.xry

Table 32

Limitations of Linear Processing

What HstEx cannot do is recover data that traverses a cluster boundary on non-contiguous clusters. This is one of the reasons why you need to also extract and examine the available live data.

Record Based Extraction (RBE)

With many of the browser types, HstEx uses a powerful search engine which is capable of Record Based Extraction.

In some circumstances, there can be limitations with RBE. Some live browser files contain information that cannot be recovered using RBE. For example, Microsoft Internet Explorer cache records contain an integer representing a zero based index which identifies the location of the cached item. Whilst the index is contained within the record, the folder array containing the folder

name string is stored at the start of the file. RBE will not recover the name of the folder as it is not stored within the record.

File Based Extraction (FBE)

Another extraction methodology employed by HstEx is File Based Extraction. Some browser index files are designed in such a way as to make RBE impossible. The History file from Firefox v1 - 2 is one such example. Firefox v1 - 2 uses a Mork database which, because of its complicated structure, makes RBE impossible. As such, it is not possible to recover individual Mork entries from unallocated clusters. In this case, HstEx employs FBE to recover Firefox v1 - 2 History.

Recommended Forensic Methodology

We recommend that you extract the live data from your source as well as processing the entire image so that you recover potentially fragmented live files and all the recoverable deleted data.

This is because:

- HstEx employs a mixture of Record (RBE) and File Based Extraction (FBE)
- Fragmented data cannot be recovered with Linear Processing
- HstEx does not support all the data types supported by NetAnalysis
- NTFS compressed data is not processed at sector level

Of course, you will end up with some duplication during your examination, but this is a small price to pay to ensure that you have all the possible evidence.

You will also need to recover live cache files for processing so that NetAnalysis can rebuild the visited pages. Internet Explorer cache entries have an index value which points to a zero based string array which stores the cache folder name. This is stored at the front of the file. This means you have to import a live cache INDEX.DAT file to get the full original path of the cache object.

During RBE extraction used by HstEx, although we can identify the index value for the array, we do not have the string array containing the folder names; therefore it is not possible to identify full cached paths using Record Based Extraction. This is why you must use both methods for a full examination.

HstEx: A Guided Tour

HstEx

To get the most from the software it is important to understand the user interface and know what each feature does. In this chapter, we will look at the various components of the user interface and understand how they work.

Main User Interface

This is the main HstEx interface with the main elements and buttons numbered for ease of identification.

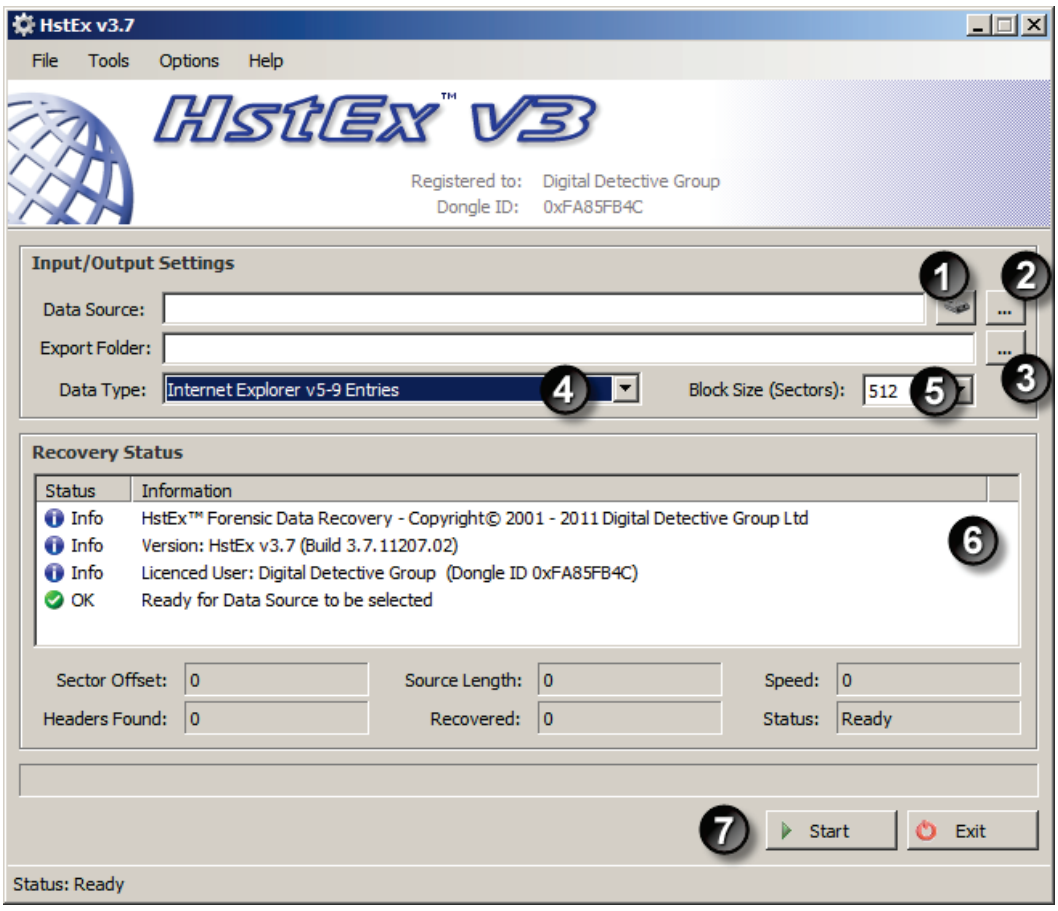


Figure 147

Table 33 explains each numbered item from Figure 147 above.

Number	Description
1	This button launches the Physical / Logical Device window and allows the forensic examiner to select any supported devices connected to the system (including removable devices).
2	This button launches the file selection window and allows the forensic examiner to select a file from which to recover data. This may be any file based container such as a forensic image or binary dump.
3	This button launches the export folder window and allows the forensic examiner to select the folder which will store the recovered browser data.
4	This drop down list allows the forensic examiner to select which type of browser related data they wish to recover.
5	This drop down list allows the forensic examiner to set the block size that HstEx will use to read and search for data. The default block size is 512 sectors (262,144 bytes).
6	This area contains a log of the recovery status and display information during the recovery.
7	This is the start button which will launch the recovery process.

Table 33

Figure 148 shows the 'Physical / Logical Devices' window. Items 0 to 4 are physical devices, whereas items C to G are logical devices. Volume F is a removable device.

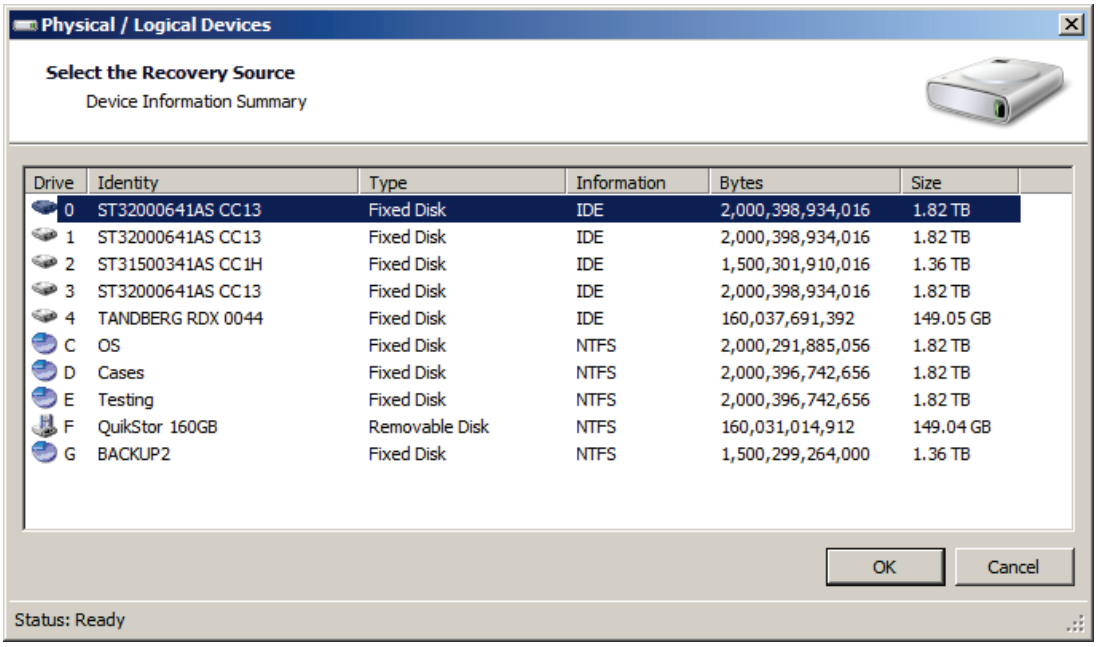


Figure 148

HstEx Quick Start

Before You Start

Prior to extracting any data, or in fact, dealing with live evidence, please ensure you have read the following chapters (as shown in Table 34).

Chapter Title	Page Number
Introduction to HstEx™	10
Installing HstEx	37
Installing a Licence Key File	44
USB Hardware Dongles	45
Practice Files	49
Deleted Data Recovery	137
HstEx: A Guided Tour	140

Table 34

We have provided a practice image to allow you to see how HstEx works; it is recommended you become familiar with the software through using the sample image and running HstEx against your own disk before accessing live evidence.

To download the practice image file, please follow the instructions on Page 49.

Getting Started

Now we have obtained the practice file set, we will use HstEx to process an EnCase® evidence file (e01). This image file is of a formatted volume which belonged to the Victor BUSHELL laptop. It has been formatted to highlight the recovery capabilities of HstEx.

Step 1

Select the image file '2011-10-19-Sample.E01' as the Data Source.

Step 2

Select the folder where you want HstEx to recover the data to.

Step 3

Select 'Internet Explorer v5-9 Entries' as the Data Type. BUSHELL was using Microsoft Internet Explorer.

Step 4

Set the Block Size (Sectors) to 512.

You can confirm the settings by comparing HstEx with Figure 149 below. If you have correctly set all of the required parameters, you are now ready to click start.

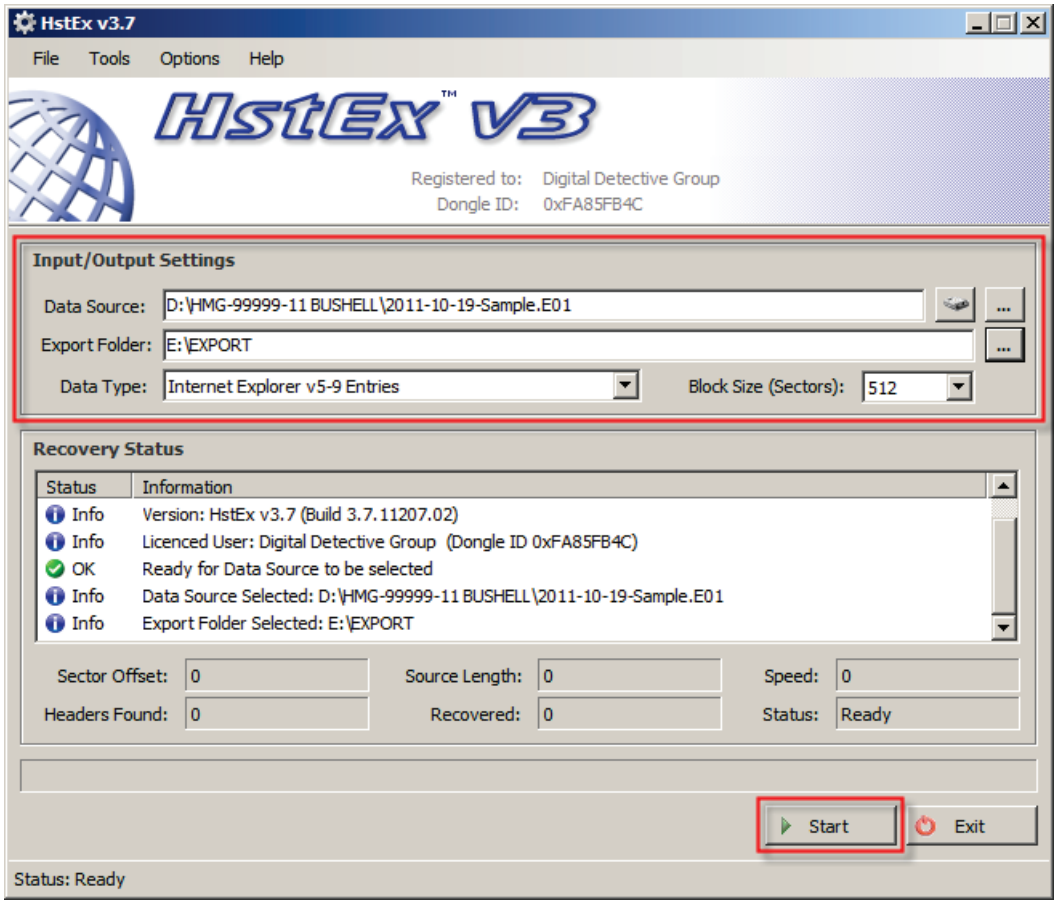


Figure 149

When the recovery process is started, HstEx will process the data in two passes. During pass one, the software will identify the location of each possible data fragment. HstEx uses sophisticated data recovery techniques to ensure that records which traverse block boundaries are not missed.

At the end of pass one, HstEx examines the locations for each fragment and removes any duplicates.

During pass two, the data is recovered, validated and then written out to our proprietary HstEx Recovery Files (HSTX). As the output format is proprietary, it cannot be opened in any other software. Figure 150 shows HstEx at the end of the recovery process.

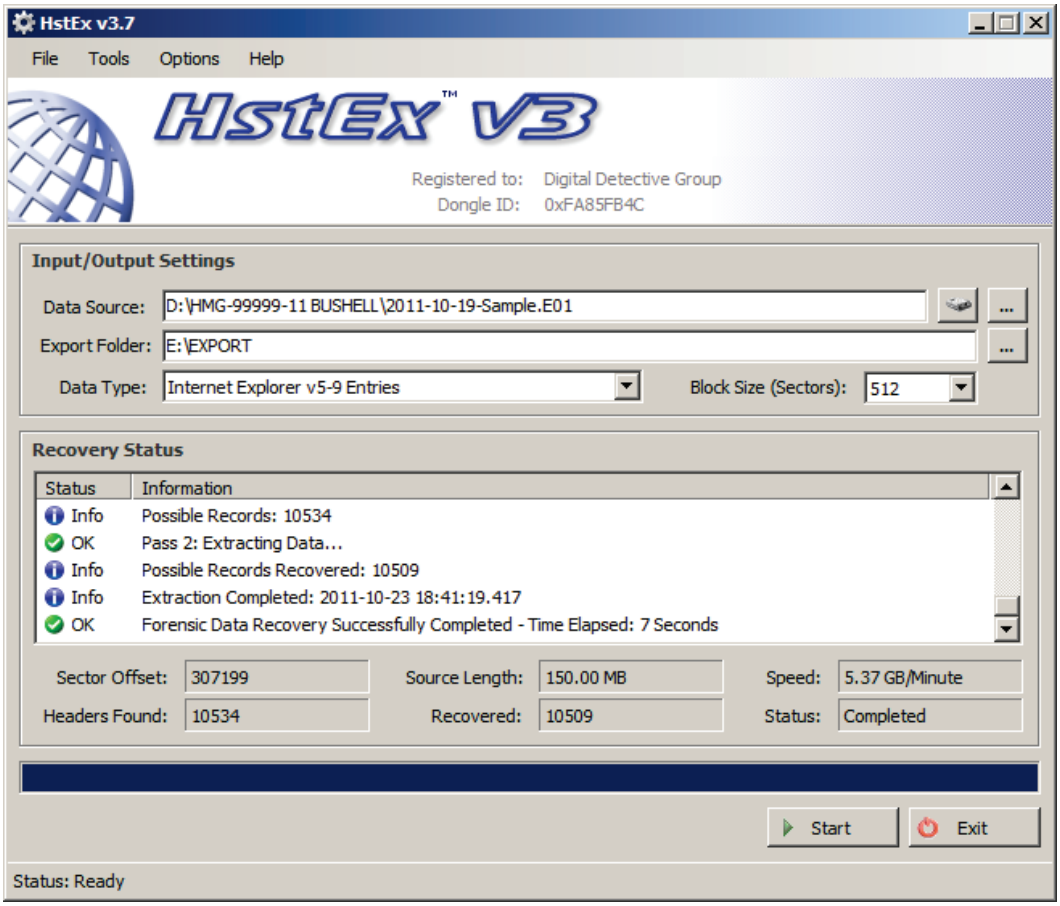


Figure 150

If the Open Export Folder on Completion option has been set (Options » Open Export Folder on Completion), HstEx will open the export folder for review.

Inside the export folder, there will be a folder relating to the evidence item processed. Inside that folder will be a session folder which contains the recovered data (if any) inside a type specific folder and the recovery log.

As each session is written to a different folder, it is possible to run the extraction process multiple times with the same export folder. Figure 151 shows our export folder containing the recovery log and Internet Explorer output folder.

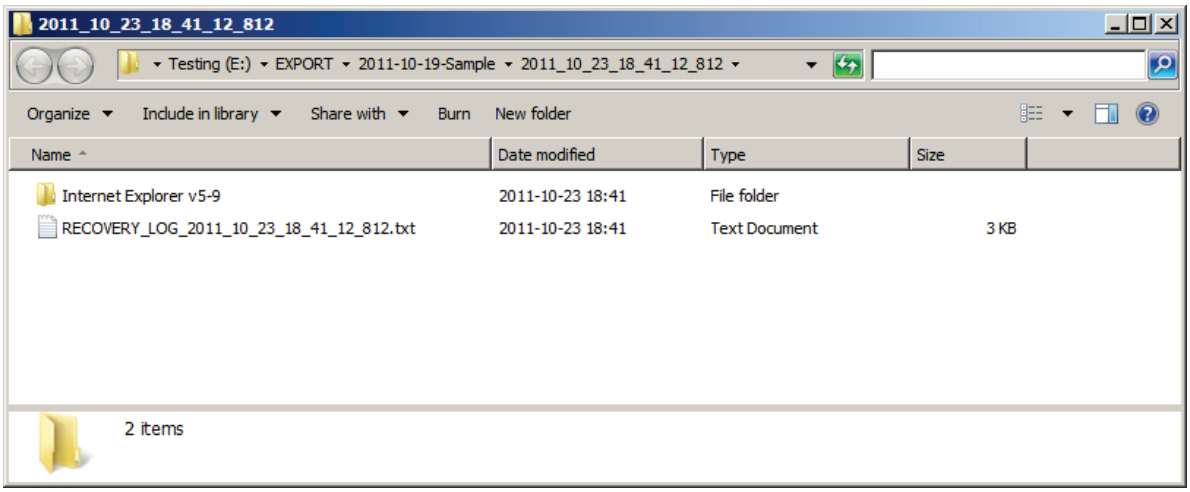


Figure 151

The output from HstEx can be imported into NetAnalysis using the Open all History from Folder method (File » Open All History from Folder), or as individual files (File » Open History). When importing as individual files, make sure you select all of the files.

In our scenario, HstEx recovered a potential 10,509 records and exported them to a single HstEx Recovery File (as shown in Figure 152).

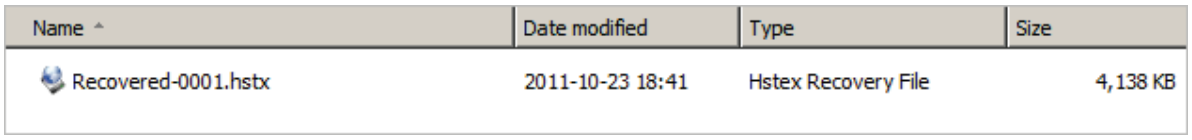


Figure 152

When HstEx writes out the recovered data, each file is capped at 5 MiB as each container may contain thousands of individual records.

Figure 153 shows the HstEx Recovery File loaded into NetAnalysis. As the original source for this data was an EnCase® evidence file, we can see highlighted the original file path for the source image as well as the physical sector and sector offset for the recovered record.

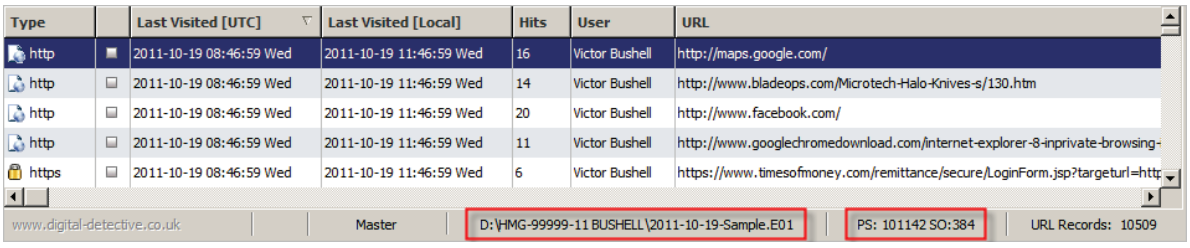


Figure 153

The path and source offset for the record are shown in the status bar for convenience; they are also recorded in the corresponding workspace fields shown in the grid.

Log File

As mentioned earlier in this chapter, HstEx writes a recovery log file to the session folder during the recovery.

Figure 154 shows the log file for this particular recovery session. The log file is a plain text file in which every entry is time stamped. It contains information such as:

- Software version and build information
- Operating system information
- Licence information
- Data source and export information

HstEx also extracts and logs the metadata information stored within the EnCase® evidence file.

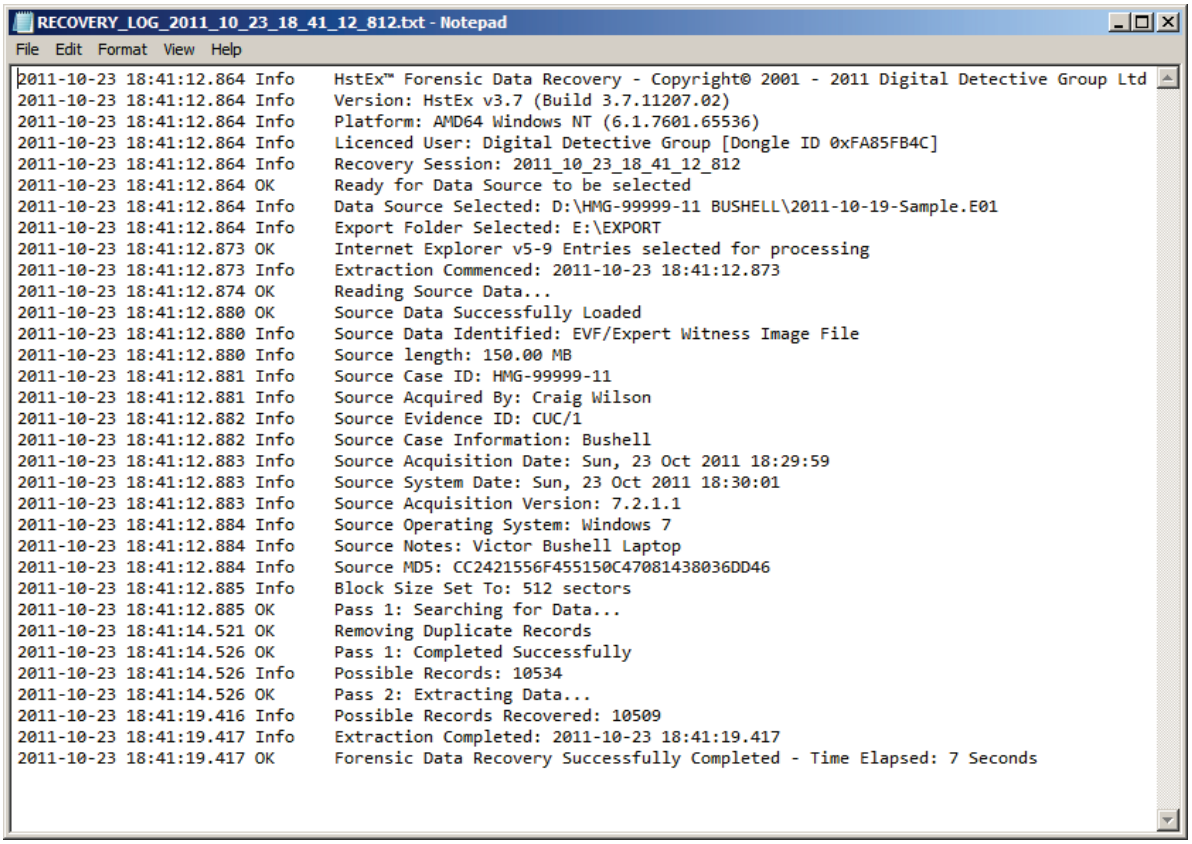


Figure 154

HstEx Options

HstEx has a number of options which can be set easily from the Options menu. They are as follows:

Options » Group Digits

This option sets whether the digits are grouped in the logs and user interface. For ease of review, numbers with many digits before the decimal mark are divided into groups using a delimiter, with the counting of groups starting from the decimal mark. This delimiter is usually called a thousands separator, because the digits are usually in groups of three (thousands).

The most general name for this delimiter is “digit group separator”, because thousands are not always the relevant group. For example, in various countries (e.g., China, India, and Japan), there have been traditional conventions of grouping by 2 or 4 digits. These conventions are still observed in some contexts, although the 3-digit group convention is also well known and often used.

Figure 155 shows the user interface with ‘Group Digits’ deactivated. Figure 156 shows the user interface with ‘Group Digits’ activated.

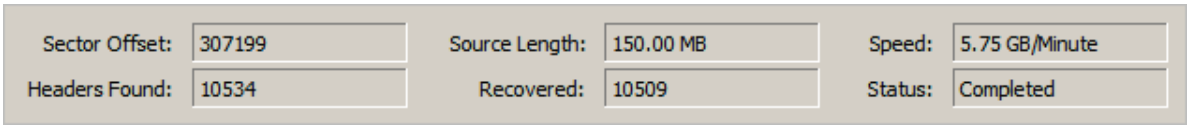


Figure 155

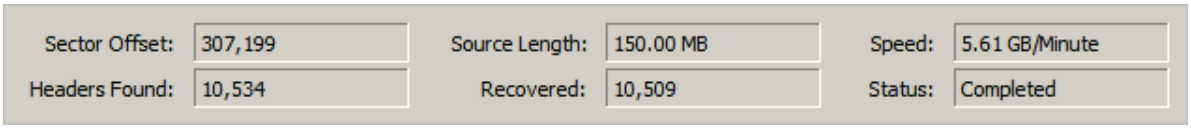


Figure 156

Options » Open Export Folder on Completion

This option allows the export folder to be automatically opened at the end of the recovery session. This option is ON by default.

The export folder can also be opened by selecting Tools » Open Export Folder (or by pressing the shortcut key CTRL+E).

Options » Force System Shutdown on Completion

This option, when set, will force a system shutdown at the end of a recovery session. It was added so that the system could be shutdown, when left unattended, when the recovery process had completed. This option is OFF by default. When the shutdown is activated (at the end of the

recovery), you have 2 minutes to cancel the shutdown if required. The shutdown can be cancelled by typing the abort command into a command prompt (as shown in Figure 157).

```
Shutdown /a
```

Figure 157

When the option is activated, a warning message is displayed underneath the progress bar (as shown in Figure 158).

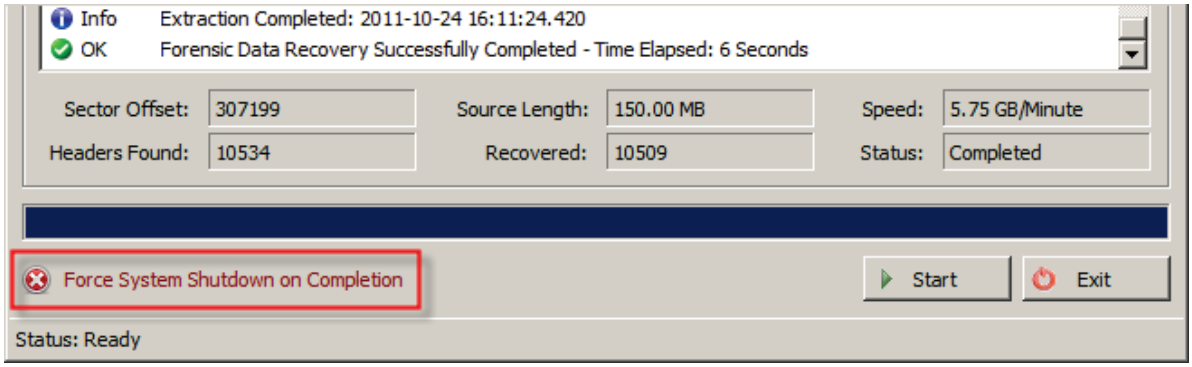


Figure 158

This option will force the operating system to shutdown at the completion of the recovery. You have two minutes to cancel the shutdown via the command line. Only use this option when you are sure that shutting down the system will not cause any issues.

Technical Support

Introduction

When seeking assistance with our software, it is extremely important that you provide enough information to allow us to understand, and potentially recreate the problem. Trying to remotely diagnose a problem is extremely difficult, particularly when we cannot have access your original data. Please be patient, and try and provide as much information as possible. To assist in the process, please read the following section prior to submitting any support ticket. Please remember to let us know if we managed to assist you.

Our support portal provides a dedicated issue management system. Whether you sign in to our support portal or send an email to our support email address, the result is the same. A new issue will be created in our database and a notification is sent to our software engineers. You will automatically receive an email notifying you of the unique reference number. If you choose to respond to our queries via email, please ensure you do not change the subject line. This means that the issue progress can be automatically tracked in our database.

Prior to submitting an issue, please open the 'About' window (as shown in Figure 159, this can be found by selecting Help » About from the menu) and identify the following:

- Software Version and Build
- Platform Information
- Licence or Dongle ID

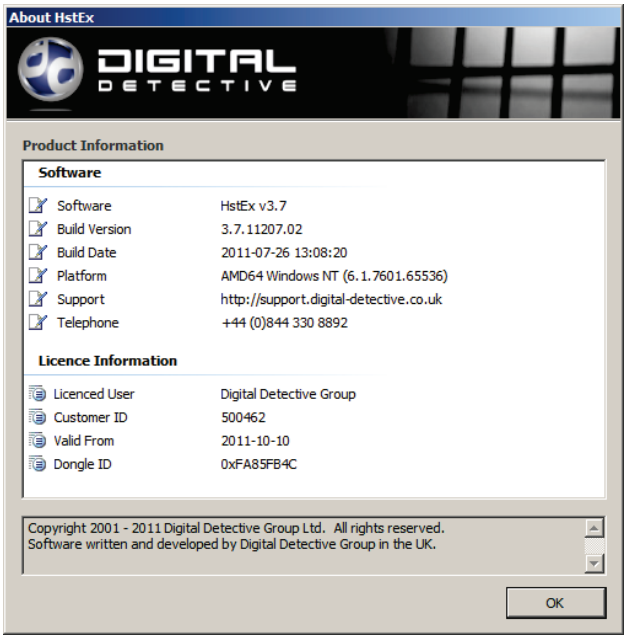


Figure 159

Submitting a Bug Report

The aim of a bug report is to enable a software engineer to identify a specific issue with the software and to establish what needs to be done to rectify the issue. To enable them to do this, you must provide careful and detailed instructions on how to make the software fail.

If they cannot replicate your issue, they will try to gather extra information until they understand the cause. If they can't make it fail, they will have to ask you to gather that information for them.

Please remember, your hardware/software setup may be completely different from our test environments and the way you use our software may also be completely different. Other software products that have been incorrectly installed by the installation/setup programme can also have a detrimental effect on our software. We use a number of shared Microsoft libraries, which if incorrectly installed or changed by another product, can cause issues. These errors are very difficult to track down, so please be patient. We will try everything we can to get our software working within your environment.

Background Information

There are three elements to a bug report:

- What you did;
- What you wanted to happen;
- What actually happened.

The most important element will be to provide step by step instructions to recreate the issue. This will allow us to recreate the bug, and put us in a much better position to rectify the problem and fix it in a future release. Use screen captures if you can; these will help the engineer to understand what you are trying to explain. Data and screen captures can be uploaded and attached to the issue in the web support portal. Getting access to the data causing the issue is also very important. This is sometimes the only way to recreate a problem.

Single line submissions such as “It won’t work” do not provide us with any useful information and will not allow an engineer to diagnose the problem. This will not help you in trying to get the software to work and the problem resolved as quickly as possible.

Check Version History

Prior to submitting a bug report or request, please review the release history for the software. This could save you time by checking to see if the issue you have has already been identified and resolved. Please also ensure you are using the latest release of our software.

If you have encountered two bugs that don't appear to be related, create a new bug report for each one. This makes it easier for different people to help with the different bugs.

The software version history and release notes can be found in our knowledge base at:

- NetAnalysis: *http://kb.digital-detective.co.uk/x/LYUU*
- HstEx: *http://kb.digital-detective.co.uk/x/oIAU*

Mandatory Information

There are a number of things that we will need from you to effectively deal with your issue. They are as follows:

Mandatory Requirements
Licence ID or USB Dongle ID
Software Version and Build Numbers
Operating System Version Information with Service Pack and Architecture Information (32/64 bit)

Table 35

NetAnalysis Error Log

If NetAnalysis encounters an error, it will write out an error log to assist with identifying the problem. The error log can be found by selecting Help » Error Reporting from the main menu. A window will open (as shown in Figure 160) showing any error log files. Please attach these logs when submitting a report.

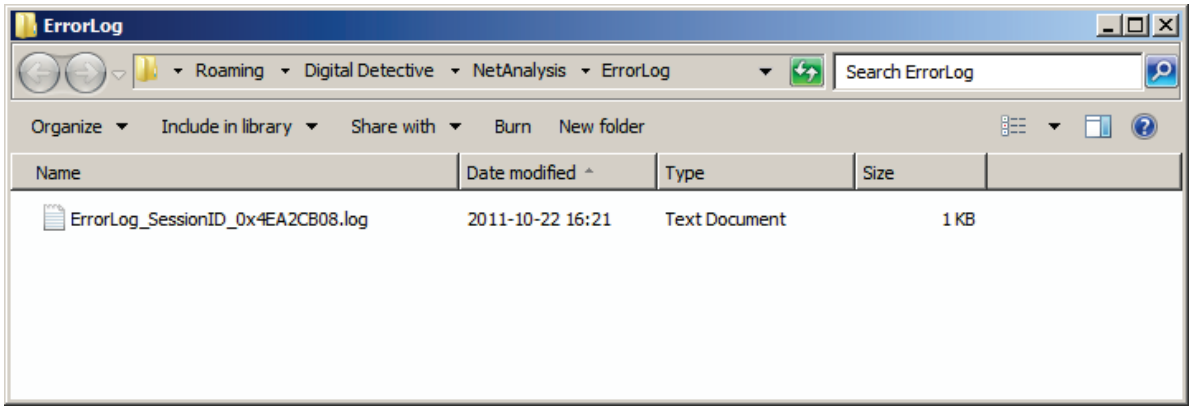


Figure 160

If you encounter a problem with HstEx, please also submit the recovery log.

Submitting an Issue

Our support portal provides a way to submit technical support requests or bug reports. Figure 161 shows the submission screen from our support system.

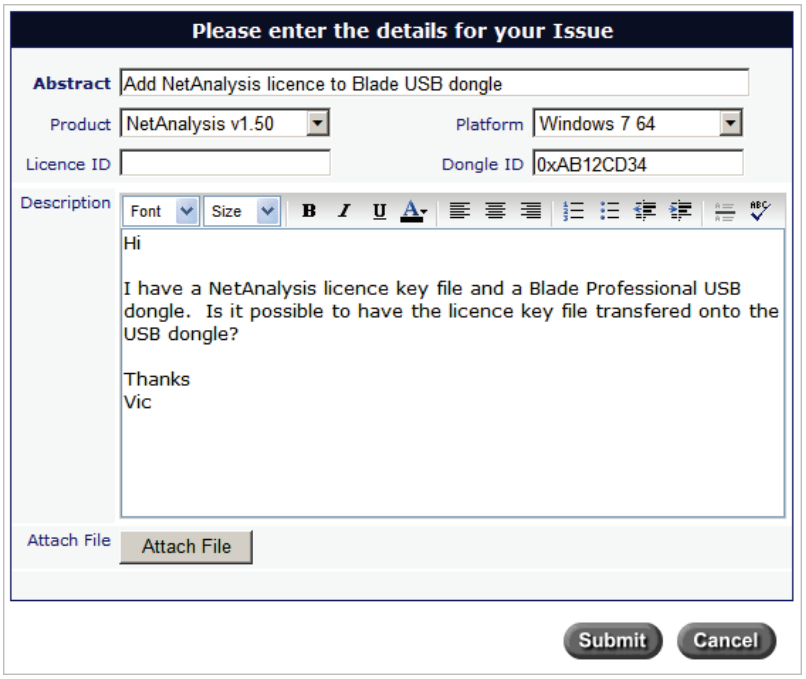


Figure 161

Figure 162 shows the submitted issue with corresponding Issue ID.

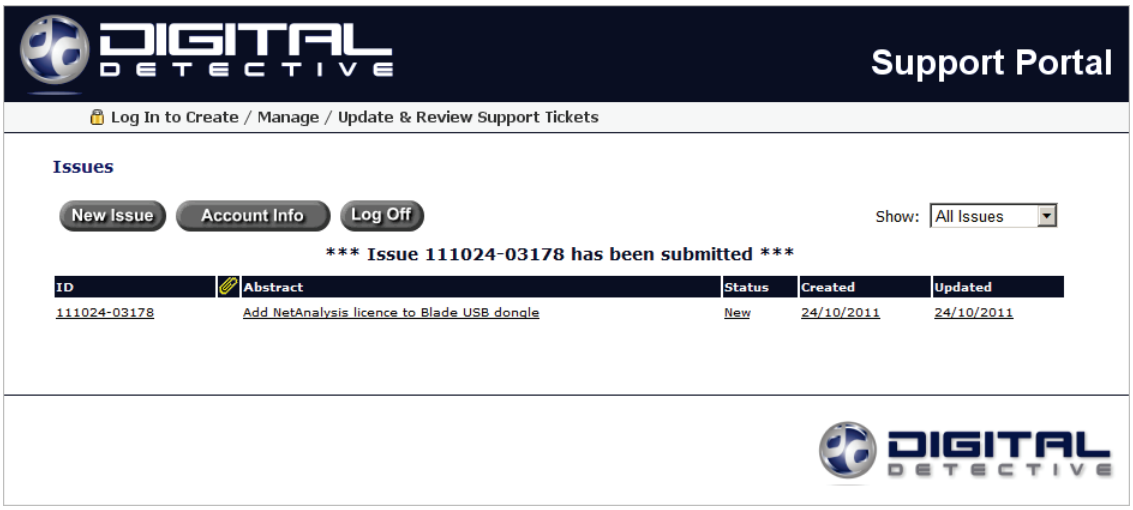


Figure 162

Once the issue has been submitted, you will receive a confirmation e-mail with a unique reference number. You can either respond to the submission via e-mail, or click in on the hyperlink (as shown in Figure 163) to take you back into the support system.

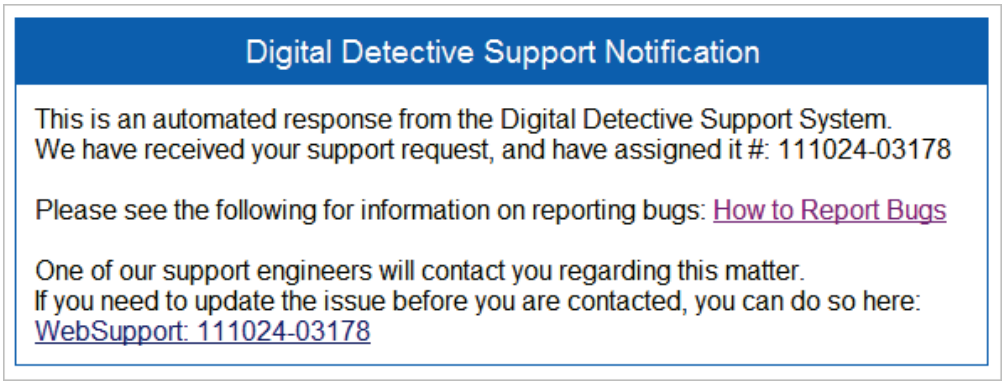


Figure 163

You can log in to the system at any time to review the response or add additional information and attachments.

Appendix A

Keyboard Shortcuts

Table 36 lists the available keyboard shortcuts.

Shortcut Key	Action Description
Space Bar	Tag Record
F2	Find Next Tagged Record
Shift + F2	Find Previous Tagged Record
F3	Find Next URL
F4	Show User Keyword List
Ctrl + F4	Show SQL Query Builder window
F5	Remove All Filters (Show All)
F6	Execute Keyword List Search - URL
Ctrl + F6	Execute SQL Query
F7	Show Find First URL Dialogue
F8	Show Filter Dialogue
F9	Filter Tagged URLs
Ctrl + F9	Filter Tagged URLs with Bookmarks
F12	Filter Live Web Pages
Ctrl + F12	Filter Live Cache Entries
Ctrl + O	Open History
Ctrl + S	Save Workspace
Ctrl + R	Preview Advanced Report
Ctrl + F5	Autosize Columns to Data

Table 36

Appendix B

Extended ASCII Table

Table 37 shows the extended ASCII character set with corresponding values.

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
0	000	00	00000000	NUL	&#000;		Null char
1	001	01	00000001	SOH	&#001;		Start of Heading
2	002	02	00000010	STX	&#002;		Start of Text
3	003	03	00000011	ETX	&#003;		End of Text
4	004	04	00000100	EOT	&#004;		End of Transmission
5	005	05	00000101	ENQ	&#005;		Enquiry
6	006	06	00000110	ACK	&#006;		Acknowledgment
7	007	07	00000111	BEL	&#007;		Bell
8	010	08	00001000	BS	&#008;		Back Space
9	011	09	00001001	HT			Horizontal Tab
10	012	0A	00001010	LF
	Line Feed
11	013	0B	00001011	VT	&#011;		Vertical Tab
12	014	0C	00001100	FF			Form Feed
13	015	0D	00001101	CR
	Carriage Return
14	016	0E	00001110	SO	&#014;		Shift Out / X-On
15	017	0F	00001111	SI	&#015;		Shift In / X-Off
16	020	10	00010000	DLE	&#016;		Data Line Escape
17	021	11	00010001	DC1	&#017;		Device Control 1 (oft. XON)
18	022	12	00010010	DC2	&#018;		Device Control 2
19	023	13	00010011	DC3	&#019;		Device Control 3 (oft. XOFF)
20	024	14	00010100	DC4	&#020;		Device Control 4
21	025	15	00010101	NAK	&#021;		Negative Acknowledgement
22	026	16	00010110	SYN	&#022;		Synchronous Idle
23	027	17	00010111	ETB	&#023;		End of Transmit Block
24	030	18	00011000	CAN	&#024;		Cancel
25	031	19	00011001	EM	&#025;		End of Medium
26	032	1A	00011010	SUB	&#026;		Substitute

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
27	033	1B	00011011	ESC	&#027;		Escape
28	034	1C	00011100	FS	&#028;		File Separator
29	035	1D	00011101	GS	&#029;		Group Separator
30	036	1E	00011110	RS	&#030;		Record Separator
31	037	1F	00011111	US	&#031;		Unit Separator
32	040	20	00100000		&#32;		Space
33	041	21	00100001	!	&#33;		Exclamation mark
34	042	22	00100010	"	&#34;	&quot;	Double quotes (or speech marks)
35	043	23	00100011	#	&#35;		Hash (or pound)
36	044	24	00100100	$	&#36;		Dollar
37	045	25	00100101	%	&#37;		Percent
38	046	26	00100110	&	&#38;	&amp;	Ampersand
39	047	27	00100111	'	&#39;		Single quote
40	050	28	00101000	(	&#40;		Open parenthesis (or open bracket)
41	051	29	00101001	)	&#41;		Close parenthesis (or close bracket)
42	052	2A	00101010	*	&#42;		Asterisk
43	053	2B	00101011	+	&#43;		Plus
44	054	2C	00101100	,	&#44;		Comma
45	055	2D	00101101	-	&#45;		Hyphen
46	056	2E	00101110	.	&#46;		Period, dot or full stop
47	057	2F	00101111	/	&#47;		Slash or divide
48	060	30	00110000	0	&#48;		Zero
49	061	31	00110001	1	&#49;		One
50	062	32	00110010	2	&#50;		Two
51	063	33	00110011	3	&#51;		Three
52	064	34	00110100	4	&#52;		Four
53	065	35	00110101	5	&#53;		Five
54	066	36	00110110	6	&#54;		Six
55	067	37	00110111	7	&#55;		Seven
56	070	38	00111000	8	&#56;		Eight
57	071	39	00111001	9	&#57;		Nine
58	072	3A	00111010	:	&#58;		Colon
59	073	3B	00111011	;	&#59;		Semicolon
60	074	3C	00111100	<	&#60;	&lt;	Less than (or open angled bracket)
61	075	3D	00111101	=	&#61;		Equals

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
62	076	3E	00111110	>	>	>	Greater than (or close angled bracket)
63	077	3F	00111111	?	?		Question mark
64	100	40	01000000	@	@		At symbol
65	101	41	01000001	A	A		Uppercase A
66	102	42	01000010	B	B		Uppercase B
67	103	43	01000011	C	C		Uppercase C
68	104	44	01000100	D	D		Uppercase D
69	105	45	01000101	E	E		Uppercase E
70	106	46	01000110	F	F		Uppercase F
71	107	47	01000111	G	G		Uppercase G
72	110	48	01001000	H	H		Uppercase H
73	111	49	01001001	I	I		Uppercase I
74	112	4A	01001010	J	J		Uppercase J
75	113	4B	01001011	K	K		Uppercase K
76	114	4C	01001100	L	L		Uppercase L
77	115	4D	01001101	M	M		Uppercase M
78	116	4E	01001110	N	N		Uppercase N
79	117	4F	01001111	O	O		Uppercase O
80	120	50	01010000	P	P		Uppercase P
81	121	51	01010001	Q	Q		Uppercase Q
82	122	52	01010010	R	R		Uppercase R
83	123	53	01010011	S	S		Uppercase S
84	124	54	01010100	T	T		Uppercase T
85	125	55	01010101	U	U		Uppercase U
86	126	56	01010110	V	V		Uppercase V
87	127	57	01010111	W	W		Uppercase W
88	130	58	01011000	X	X		Uppercase X
89	131	59	01011001	Y	Y		Uppercase Y
90	132	5A	01011010	Z	Z		Uppercase Z
91	133	5B	01011011	[	[		Opening bracket
92	134	5C	01011100	\	\		Backslash
93	135	5D	01011101	]	]		Closing bracket
94	136	5E	01011110	^	^		Caret - circumflex
95	137	5F	01011111	_	_		Underscore
96	140	60	01100000	`	`		Grave accent

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
97	141	61	01100001	a	&#97;		Lowercase a
98	142	62	01100010	b	&#98;		Lowercase b
99	143	63	01100011	c	&#99;		Lowercase c
100	144	64	01100100	d	&#100;		Lowercase d
101	145	65	01100101	e	&#101;		Lowercase e
102	146	66	01100110	f	&#102;		Lowercase f
103	147	67	01100111	g	&#103;		Lowercase g
104	150	68	01101000	h	&#104;		Lowercase h
105	151	69	01101001	i	&#105;		Lowercase i
106	152	6A	01101010	j	&#106;		Lowercase j
107	153	6B	01101011	k	&#107;		Lowercase k
108	154	6C	01101100	l	&#108;		Lowercase l
109	155	6D	01101101	m	&#109;		Lowercase m
110	156	6E	01101110	n	&#110;		Lowercase n
111	157	6F	01101111	o	&#111;		Lowercase o
112	160	70	01110000	p	&#112;		Lowercase p
113	161	71	01110001	q	&#113;		Lowercase q
114	162	72	01110010	r	&#114;		Lowercase r
115	163	73	01110011	s	&#115;		Lowercase s
116	164	74	01110100	t	&#116;		Lowercase t
117	165	75	01110101	u	&#117;		Lowercase u
118	166	76	01110110	v	&#118;		Lowercase v
119	167	77	01110111	w	&#119;		Lowercase w
120	170	78	01111000	x	&#120;		Lowercase x
121	171	79	01111001	y	&#121;		Lowercase y
122	172	7A	01111010	z	&#122;		Lowercase z
123	173	7B	01111011	{	&#123;		Opening brace
124	174	7C	01111100	|	&#124;		Vertical bar
125	175	7D	01111101	}	&#125;		Closing brace
126	176	7E	01111110	~	&#126;		Equivalency sign - tilde
127	177	7F	01111111		&#127;		Delete
128	200	80	10000000	€	&#128;	&euro;	Euro sign
129	201	81	10000001				
130	202	82	10000010	‚	&#130;	&sbquo;	Single low-9 quotation mark
131	203	83	10000011	ƒ	&#131;	&fnof;	Latin small letter f with hook

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
132	204	84	10000100	„	„	„	Double low-9 quotation mark
133	205	85	10000101	…	…	…	Horizontal ellipsis
134	206	86	10000110	†	†	†	Dagger
135	207	87	10000111	‡	‡	‡	Double dagger
136	210	88	10001000	ˆ	ˆ	ˆ	Modifier letter circumflex accent
137	211	89	10001001	‰	‰	‰	Per mille sign
138	212	8A	10001010	Š	Š	Š	Latin capital letter S with caron
139	213	8B	10001011	‹	‹	‹	Single left-pointing angle quotation
140	214	8C	10001100	Œ	Œ	Œ	Latin capital ligature OE
141	215	8D	10001101				
142	216	8E	10001110	Ž	Ž		Latin capital letter Z with caron
143	217	8F	10001111				
144	220	90	10010000				
145	221	91	10010001	‘	‘	‘	Left single quotation mark
146	222	92	10010010	’	’	’	Right single quotation mark
147	223	93	10010011	“	“	“	Left double quotation mark
148	224	94	10010100	”	”	”	Right double quotation mark
149	225	95	10010101	•	•	•	Bullet
150	226	96	10010110	–	–	–	En dash
151	227	97	10010111	—	—	—	Em dash
152	230	98	10011000	˜	˜	˜	Small tilde
153	231	99	10011001	™	™	™	Trade mark sign
154	232	9A	10011010	š	š	š	Latin small letter S with caron
155	233	9B	10011011	›	›	›	Single right-pointing angle quotation mark
156	234	9C	10011100	œ	œ	œ	Latin small ligature oe
157	235	9D	10011101				
158	236	9E	10011110	ž	ž		Latin small letter z with caron
159	237	9F	10011111	Ÿ	Ÿ	ÿ	Latin capital letter Y with diaeresis
160	240	A0	10100000				Non-breaking space
161	241	A1	10100001	¡	¡	¡	Inverted exclamation mark
162	242	A2	10100010	¢	¢	¢	Cent sign
163	243	A3	10100011	£	£	£	Pound sign
164	244	A4	10100100	¤	¤	¤	Currency sign
165	245	A5	10100101	¥	¥	¥	Yen sign
166	246	A6	10100110	¦	¦	¦	Pipe, Broken vertical bar

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
167	247	A7	10100111	§	§	§	Section sign
168	250	A8	10101000	¨	¨	¨	Spacing diaeresis - umlaut
169	251	A9	10101001	©	©	©	Copyright sign
170	252	AA	10101010	ª	ª	ª	Feminine ordinal indicator
171	253	AB	10101011	«	«	«	Left double angle quotes
172	254	AC	10101100	¬	¬	¬	Not sign
173	255	AD	10101101				Soft hyphen
174	256	AE	10101110	®	®	®	Registered trade mark sign
175	257	AF	10101111	¯	¯	¯	Spacing macron - overline
176	260	B0	10110000	°	°	°	Degree sign
177	261	B1	10110001	±	±	±	Plus-or-minus sign
178	262	B2	10110010	²	²	²	Superscript two - squared
179	263	B3	10110011	³	³	³	Superscript three - cubed
180	264	B4	10110100	´	´	´	Acute accent - spacing acute
181	265	B5	10110101	µ	µ	µ	Micro sign
182	266	B6	10110110	¶	¶	¶	Pilcrow sign - paragraph sign
183	267	B7	10110111	·	·	·	Middle dot - Georgian comma
184	270	B8	10111000	¸	¸	¸	Spacing cedilla
185	271	B9	10111001	¹	¹	¹	Superscript one
186	272	BA	10111010	º	º	º	Masculine ordinal indicator
187	273	BB	10111011	»	»	»	Right double angle quotes
188	274	BC	10111100	¼	¼	¼	Fraction one quarter
189	275	BD	10111101	½	½	½	Fraction one half
190	276	BE	10111110	¾	¾	¾	Fraction three quarters
191	277	BF	10111111	¿	¿	¿	Inverted question mark
192	300	C0	11000000	À	À	À	Latin capital letter A with grave
193	301	C1	11000001	Á	Á	Á	Latin capital letter A with acute
194	302	C2	11000010	Â	Â	Â	Latin capital letter A with circumflex
195	303	C3	11000011	Ã	Ã	Ã	Latin capital letter A with tilde
196	304	C4	11000100	Ä	Ä	Ä	Latin capital letter A with diaeresis
197	305	C5	11000101	Å	Å	Å	Latin capital letter A with ring above
198	306	C6	11000110	Æ	Æ	Æ	Latin capital letter AE
199	307	C7	11000111	Ç	Ç	Ç	Latin capital letter C with cedilla
200	310	C8	11001000	È	È	È	Latin capital letter E with grave
201	311	C9	11001001	É	É	É	Latin capital letter E with acute

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
202	312	CA	11001010	Ê	Ê	Ê	Latin capital letter E with circumflex
203	313	CB	11001011	Ë	Ë	Ë	Latin capital letter E with diaeresis
204	314	CC	11001100	Ì	Ì	Ì	Latin capital letter I with grave
205	315	CD	11001101	Í	Í	Í	Latin capital letter I with acute
206	316	CE	11001110	Î	Î	Î	Latin capital letter I with circumflex
207	317	CF	11001111	Ï	Ï	Ï	Latin capital letter I with diaeresis
208	320	D0	11010000	Ð	Ð	Ð	Latin capital letter ETH
209	321	D1	11010001	Ñ	Ñ	Ñ	Latin capital letter N with tilde
210	322	D2	11010010	Ò	Ò	Ò	Latin capital letter O with grave
211	323	D3	11010011	Ó	Ó	Ó	Latin capital letter O with acute
212	324	D4	11010100	Ô	Ô	Ô	Latin capital letter O with circumflex
213	325	D5	11010101	Õ	Õ	Õ	Latin capital letter O with tilde
214	326	D6	11010110	Ö	Ö	Ö	Latin capital letter O with diaeresis
215	327	D7	11010111	×	×	×	Multiplication sign
216	330	D8	11011000	Ø	Ø	Ø	Latin capital letter O with slash
217	331	D9	11011001	Ù	Ù	Ù	Latin capital letter U with grave
218	332	DA	11011010	Ú	Ú	Ú	Latin capital letter U with acute
219	333	DB	11011011	Û	Û	Û	Latin capital letter U with circumflex
220	334	DC	11011100	Ü	Ü	Ü	Latin capital letter U with diaeresis
221	335	DD	11011101	Ý	Ý	Ý	Latin capital letter Y with acute
222	336	DE	11011110	Þ	Þ	Þ	Latin capital letter THORN
223	337	DF	11011111	ß	ß	ß	Latin small letter sharp s - ess-zed
224	340	E0	11100000	à	à	à	Latin small letter a with grave
225	341	E1	11100001	á	á	á	Latin small letter a with acute
226	342	E2	11100010	â	â	â	Latin small letter a with circumflex
227	343	E3	11100011	ã	ã	ã	Latin small letter a with tilde
228	344	E4	11100100	ä	ä	ä	Latin small letter a with diaeresis
229	345	E5	11100101	å	å	å	Latin small letter a with ring above
230	346	E6	11100110	æ	æ	æ	Latin small letter ae
231	347	E7	11100111	ç	ç	ç	Latin small letter c with cedilla
232	350	E8	11101000	è	è	è	Latin small letter e with grave
233	351	E9	11101001	é	é	é	Latin small letter e with acute
234	352	EA	11101010	ê	ê	ê	Latin small letter e with circumflex
235	353	EB	11101011	ë	ë	ë	Latin small letter e with diaeresis
236	354	EC	11101100	ì	ì	ì	Latin small letter i with grave

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
237	355	ED	11101101	í	í	í	Latin small letter i with acute
238	356	EE	11101110	î	î	î	Latin small letter i with circumflex
239	357	EF	11101111	ï	ï	ï	Latin small letter i with diaeresis
240	360	F0	11110000	ð	ð	ð	Latin small letter eth
241	361	F1	11110001	ñ	ñ	ñ	Latin small letter n with tilde
242	362	F2	11110010	ò	ò	ò	Latin small letter o with grave
243	363	F3	11110011	ó	ó	ó	Latin small letter o with acute
244	364	F4	11110100	ô	ô	ô	Latin small letter o with circumflex
245	365	F5	11110101	õ	õ	õ	Latin small letter o with tilde
246	366	F6	11110110	ö	ö	ö	Latin small letter o with diaeresis
247	367	F7	11110111	÷	÷	÷	Division sign
248	370	F8	11111000	ø	ø	ø	Latin small letter o with slash
249	371	F9	11111001	ù	ù	ù	Latin small letter u with grave
250	372	FA	11111010	ú	ú	ú	Latin small letter u with acute
251	373	FB	11111011	û	û	û	Latin small letter u with circumflex
252	374	FC	11111100	ü	ü	ü	Latin small letter u with diaeresis
253	375	FD	11111101	ý	ý	ý	Latin small letter y with acute
254	376	FE	11111110	þ	þ	þ	Latin small letter thorn
255	377	FF	11111111	ÿ	ÿ	ÿ	Latin small letter y with diaeresis

Table 37

List of References

Reference Index

[1]. Williams, P. (2008). Organized Crime and Cybercrime: Synergies, Trends, and Responses. Retrieved March 21, 2011, from *http://www.crime-research.org/library/Cybercrime.htm*

[2]. Microsoft, (2011). Daylight Saving Time Help and Support. Retrieved October 20, 2011, from *http://support.microsoft.com/gp/cp_dst*

[3]. Microsoft, (2006). What are Control Sets? What is CurrentControlSet? Retrieved October 20, 2011, from *http://support.microsoft.com/kb/100010*